IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

	§	
	§	ORIGINAL COMPLAINT FOR
	§	VIOLATIONS OF FEDERAL
ABC,	§	FALSE CLAIMS ACT
	§	
Plaintiffs,	§	FILED UNDER SEAL
	§	PURSUANT TO 31 U.S.C.
	§	§ 3730(b)(2)
	§	
v.	§	Case No.: _____
	§	
	§	DO NOT PUT ON PACER
	§	
	§	DO NOT PLACE IN PRESS
XYZ,	§	BOX
	§	
Defendants.	§	JURY TRIAL DEMANDED
	§	

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	§	
ex rel. John Kurzman;	§	
DISTRICT OF COLUMBIA	§	
ex rel. John Kurzman;	§	
STATE OF CALIFORNIA	§	
ex. rel. John Kurzman;	§	
STATE OF DELAWARE	§	CIV. NO. _____
ex rel. John Kurzman;	§	
STATE OF FLORIDA	§	
ex rel. John Kurzman;	§	RELATOR JOHN KURZMAN'S
STATE OF HAWAII	§	ORIGINAL COMPLAINT
ex rel. John Kurzman;	§	
STATE OF ILLINOIS	§	
ex rel. John Kurzman;	§	FILED UNDER SEAL
STATE OF INDIANA	§	
ex rel. John Kurzman;	§	
STATE OF IOWA	§	JURY TRIAL DEMANDED
ex rel. John Kurzman;	§	
COMMONWEALTH OF MASSACHUSETTS	§	
ex rel. John Kurzman;	§	
STATE OF MINNESOTA	§	
ex rel. John Kurzman;	§	
STATE OF MONTANA	§	
ex rel. John Kurzman;	§	
STATE OF NEVADA	§	
ex rel. John Kurzman;	§	
STATE OF NEW JERSEY	§	
ex rel. John Kurzman;	§	
STATE OF NEW MEXICO	§	
ex rel. John Kurzman;	§	
STATE OF NORTH CAROLINA	§	
ex rel. John Kurzman;	§	
STATE OF RHODE ISLAND	§	
ex rel. John Kurzman;	§	
STATE OF TENNESSEE	§	
ex rel. John Kurzman;	§	
STATE OF VERMONT	§	
ex. rel. John Kurzman;	§	
COMMONWEALTH OF VIRGINIA	§	
ex rel. John Kurzman;	§	
CITY OF CHICAGO	§	
ex rel. John Kurzman;	§	

COUNTY OF BROWARD	§
ex rel. John Kurzman;	§
COUNTY OF MIAMI-DADE	§
ex rel. John Kurzman,	§
	§
Plaintiffs,	§
	§
v.	§
	§
MICROSOFT CORP.; MICROSOFT LICENSING, G.P.; AERIE CONSULTING, LLC; ALVAREZ & ASSOCIATES, LLC; ARCTIC INFORMATION TECHNOLOGY, INC.; CDW CORP.; CDW GOVERNMENT, LLC, F/K/A CDW GOVERNMENT, INC.; CHAMPION SOLUTIONS GROUP, INC.; COMPUCOM SYSTEMS, INC.; CORNERSTONE IT, INC.; CRAYON SOFTWARE EXPERTS LLC; DELL MARKETING, L.P.; ECS FEDERAL, LLC; EN POINTE TECHNOLOGY SALES, LLC; THE HENSON GROUP, INC.; IMAGER SOFTWARE, INC., D/B/A ISC; INFORELIANCE LLC, F/K/A INFORELIANCE CORP.; INSIGHT PUBLIC SECTOR, INC., A/K/A INSIGHT ENTERPRISES, INC.; INTRAPRISE TECHKNOWLOGIES LLC; LIFTOFF, LLC; LILIEN, LLC, A/K/A LILIEN SYSTEMS; MINBURN TECHNOLOGY GROUP LLC; PCM, INC.; PCMG, INC., D/B/A PCM GOV, INC.; PLANET TECHNOLOGIES, INC.; PROCENTRIX, INC.; PROSUM INC., A/K/A PROSUM TECHNOLOGIES; SHI INTERNATIONAL CORP., F/K/A SOFTWARE HOUSE INTERNATIONAL, INC.; SOFTCHOICE CORP.; SOFTWARE ONE, INC.; SOLID NETWORKS INC.; SYSOREX GOVERNMENT SERVICES, INC.; T4 TECHNOLOGIES, INC.; VENTECH SOLUTIONS INC.,	§
	§
Defendants.	§
	§
	§

RELATOR JOHN KURZMAN'S ORIGINAL COMPLAINT

TABLE OF CONTENTS

1. On behalf of the United States of America, the District of Columbia, the States of California, Delaware, Florida, Hawaii, Illinois, Indiana, Iowa, Minnesota, Montana, Nevada, New Jersey, New Mexico, North Carolina, Rhode Island, Tennessee, and Vermont, the Commonwealths of Virginia and Massachusetts, the City of Chicago, and the Counties of Broward and Miami-Dade, Florida (hereinafter "Government Plaintiffs"), Plaintiff/Relator John Kurzman ("Kurzman" or "Relator") brings this action pursuant to the Federal False Claims Act, 31 U.S.C. §§ 3729–3732, and the *qui tam* statutes of the above-captioned States, Commonwealths, City, Counties, and the District of Columbia, and seeks to recover all damages, penalties, and other remedies established by the federal False Claims Act and state false claims acts on behalf of the Government Plaintiffs, and on his own behalf. Relator would respectfully show the following:

I. INTRODUCTION TO CASE

2. Defendants Microsoft Corporation, Microsoft Licensing, G.P., and their licensed resellers (collectively "Defendants") defrauded the Government Plaintiffs out of hundreds of millions of dollars and put government data at risk.

3. Specifically, Defendants fraudulently induced the Government Plaintiffs and their agencies to enter into contracts and pay for cloud computing services that, contrary to Defendants' representations, do not operate exclusively within a secure "government cloud" but instead operate partially within Microsoft's general "commercial cloud." The "fake" government cloud services at issue—known as "GCC"—put government data at an increased risk of hacking.

4. Defendants worked in tandem to procure contracts, and payment under them, from the Government Plaintiffs and their agencies. Defendants Microsoft Corporation and

Microsoft Licensing, G.P. (collectively "Microsoft") do not sell products or services directly to customers. Instead, sales are made through licensed Microsoft resellers—in this case, Defendants Aerie Consulting, LLC, Alvarez & Associates, LLC, Arctic Information Technology, Inc., CDW Corporation, CDW Government, LLC, Champion Solutions Group, Inc., CompuCom Systems, Inc., Cornerstone IT, Inc., Crayon Software Experts LLC, Dell Marketing, L.P., ECS Federal, LLC, En Pointe Technologies Sales, LLC, The Henson Group, Inc., Imager Software, Inc., InfoReliance LLC, Insight Public Sector, Inc., Intraprise TechKnowlogies LLC, Liftoff, LLC, Lilien, LLC, Minburn Technology Group LLC, PCM, Inc., PCMG, Inc., Planet Technologies, Inc., Procentrix, Inc., ProSum Inc., SHI International Corporation, Softchoice Corporation, Software One, Inc., Solid Networks Inc., Sysorex Government Services, Inc., T4 Technologies, Inc., and Ventech Solutions Inc. (collectively, the "Reseller Defendants").

5. The Reseller Defendants entered into contracts with the Government Plaintiffs and their agencies for the sale of Microsoft products and services, including cloud computing products and services ("cloud services") like GCC. Concurrently, Microsoft entered into agreements with the Government Plaintiffs and their agencies as part of these contracts, including licensing agreements and business agreements.

6. In obtaining these contracts and agreements, Defendants made false statements about the cloud services at issue, via marketing material, websites, and other statements made to representatives of the Government Plaintiffs and their agencies.

7. Namely, Microsoft's marketing material emphasizes that its cloud services for government customers are exclusive to the government and operate within a segregated "government cloud." In truth, however, the cloud services at issue do not operate exclusively within a "government cloud." Instead, they operate partially within Microsoft's general

"commercial cloud", which is available to all commercial users within the United States. In fact, some of the most security-crucial parts of GCC, such as usernames and credential information for password validation and logins, reside entirely within the commercial cloud.

8. By placing security-crucial operations and information in the commercial cloud, Defendants put government data at an increased risk of breach and hacking. Because the commercial cloud is shared with non-government users, data and operations occurring even partially within the commercial cloud face an increased risk of security breach compared to a "true" government cloud, which is segregated completely from a public cloud like the commercial cloud.

9. Relying on Defendants' misrepresentations, and attracted by the security purportedly offered by GCC, the Government Plaintiffs and their agencies entered into contracts and agreements with Defendants. The contracts and agreements themselves further perpetuate Defendants' fraud, stating that the services at issue utilize a government-exclusive "government community cloud", when, in fact, they do not.

10. The deception did not end with the contracts, however. Microsoft actively hid GCC's partial use of the commercial cloud from Government Plaintiff agency customers. For example, government users' login portal for GCC appeared to be an exclusive portal for Microsoft government cloud services. But, had users attempted to log in via the "commercial" cloud portal website, they would have seen the truth—that their identities (usernames and passwords) existed in the "commercial" cloud.

11. The Government Plaintiffs have paid hundreds of millions of dollars for "fake" government cloud services that are not as secure and government-exclusive as represented.

12. Defendants have damaged the Government Plaintiffs by causing them to enter into contracts and pay claims under those contracts for cloud computing services, which they would not have done had they known that GCC was not a true "government cloud."

II. JURISDICTION AND VENUE

13. Jurisdiction and venue are proper in the Southern District of New York pursuant to the False Claims Act (31 U.S.C. § 3732(a)) because Relator's claims seek remedies on behalf of the United States for multiple violations of the federal False Claims Act, some of which occurred in the Southern District of New York. Defendants engage in business in the Southern District of New York and are subject to general and specific personal jurisdiction pursuant to 31 U.S.C. § 3732(a) in that the claims for relief in this action are brought on behalf of the United States for multiple violations of the federal False Claims Act. Pendent jurisdiction is also proper over Relator's state claims under 18 U.S.C. § 3732 and 28 U.S.C. § 1367.

III. GOVERNMENT PLAINTIFFS

14. The Government Plaintiffs in this lawsuit are: the United States of America; the District of Columbia; the States of California, Delaware, Florida, Hawaii, Illinois, Indiana, Iowa, Minnesota, Montana, Nevada, New Jersey, New Mexico, North Carolina, Rhode Island, Tennessee, and Vermont; the Commonwealths of Massachusetts and Virginia; the City of Chicago; and the Counties of Broward and Miami-Dade, Florida.

IV. INTRODUCTION TO RELATOR JOHN KURZMAN

A. Relator's Background

15. Relator John Kurzman ("Relator" or "Kurzman") is a Certified Information Systems Security Professional who has worked in information technology security for over a decade. Relator worked for Defendant Microsoft Corporation as a Security Global Black Belt

for Enterprise Mobility & Security in New York and New Jersey from January 4, 2016 until his termination in July 5, 2017, effective on September 4, 2017.

16. As a Security Global Black Belt, Relator was responsible for being knowledgeable about Microsoft's Enterprise Mobility & Security Suite and two main products within it, Azure Information Protection ("AIP")[1] and Cloud Application Security ("CAS").[2] Relator was also responsible for identifying and removing "blockers"—Microsoft's terminology for anything that prevents a sale from occurring or a contract from being signed.

17. During the relevant time period, Relator's acting supervisor was Kevin Bognar ("Bognar"), Senior Director of Solution Sales, and his direct supervisor was Amrit Pal "Roger" Singh ("Singh"), who earlier had been head of Enterprise Mobility & Security Sales for the Americas, and was later Director of Solution Sales for the Enterprise and Partner Group. Singh worked under Bognar.

18. Relator was tasked with helping to sell AIP and CAS, as part of the Enterprise Mobility & Security Suite ("EMS"), to government customers, including customers in the State and Local Government ("SLG") and Federal ("FED") sectors.

19. Relator's superiors and Microsoft's government sales teams misrepresented to Relator that federal and state government customers for GCC—Microsoft's "fake" government cloud service—were aware that their identities (i.e., usernames and other credentials) were stored in the commercial cloud.

20. While Microsoft markets a "government cloud" product that is exclusive to government users and segregated from the general commercial cloud, not all products or services operate exclusively within the government cloud. While the GCC services at issue were

[1] A complete glossary of acronyms is provided at the end of this document.
[2] Microsoft cloud product offerings are described further *infra* in greater detail.

marketed as an "exclusive" government cloud, segregated from the commercial cloud, this was not the case.

21. Relator first learned of this fact in August of 2016, but he was continually told by superiors that customers knew the truth or that the contractual language stated the truth. However, as Relator would eventually discover, this was not the case—Microsoft's deceptive marketing and representations to the Government Plaintiffs all referenced government-exclusive services and made no mention of the commercial cloud.

22. Relator reported and sought to stop security issues with GCC and EMS beginning in September 2016. Relator also reported and sought to stop deceptive marketing and statements regarding Microsoft's government cloud offerings. Relator's reports and efforts to stop fraud against the Government Plaintiffs continued up until his date of termination.

23. In January of 2017, Microsoft selected the Port Authority of New York and New Jersey ("PANYNJ") to be a "test" customer for AIP.

24. When Relator helped assist PANYNJ in the installation of AIP, PANYNJ was shocked to find that the identities of its users were stored in the commercial cloud. This initially caused difficulties, and Relator was blamed for "unselling" EMS to PANYNJ.

25. Although Relator's first employment evaluation was positive, once Relator's supervisors learned of his reports of and efforts to stop fraud, manager comments on Relator's evaluations became increasingly negative. This culminated in "Insufficient Results" notations on Relator's February and June 2017 evaluations, which made it nearly impossible for Relator to transfer to a new position within Microsoft.

26. One of Relator's last e-mails to Singh makes Defendants' fraud on the Government Plaintiffs as clear as day:

> i. [W]e SHOW CUSTOMERS THEIR IDENTITIES ARE IN THE GOV[ERNMENT] CLOUD IN THE GOV[ERNMENT] CONSOLE, WHICH IS NOT TRUE
> ii. datasheets and marketing materials and [Microsoft's website] reflect same, which is not true, comingling gcc and [Azure] defense[, the true government cloud,] information together.

Ex. 1, E-mail with Singh & Case (June 23, 2017), at 1. However, no corrective action was taken.

27. Relator's position was eliminated, as well as the positions of some other Microsoft employees, on July 6, 2017, effective September 4, 2017. All eliminated employees except for Relator were offered new positions within Microsoft. Further, Relator's "Insufficient Results" notation made it impossible for him to obtain a new position without the approval of two Microsoft Vice Presidents.

28. Between July 6, 2017 and his termination date of September 4, 2017, Relator continued to receive a salary, but did not perform any work for Microsoft. Despite his pending termination, Relator strived to bring an end to the ongoing fraud on the Government Plaintiffs, e-mailing several executives near the top of Microsoft's organizational structure about the ongoing security issues with GCC.

B. Original Source and Disclosures

29. There are no bars to recovery under 31 U.S.C. § 3730(e), or in the alternative, Relator is an original source as defined therein. Relator has direct and independent knowledge of the information on which he bases his allegations. To the extent that any allegations or transactions herein have been publicly disclosed, Relator has independent knowledge that materially adds to any publicly disclosed allegations or transactions and has provided this information to the United States and the other Government Plaintiffs prior to filing a complaint by serving a voluntary pre-filing disclosure statement on May 3, 2019.

30. As required pursuant to 31 U.S.C. § 3730(b), Relator will submit an original disclosure statement to the Attorney General of the United States and the United States Attorney for the Southern District of New York, as well as substantially all material evidence and information, contemporaneously with the service of his Original Complaint.

31. In accordance with their respective state and local *qui tam* statutes, Relator will submit an original disclosure to the Attorneys General of the District of Columbia, the States of California, Delaware, Florida, Hawaii, Illinois, Indiana, Iowa, Minnesota, Montana, Nevada, New Jersey, New Mexico, North Carolina, Rhode Island, Tennessee, and Vermont, and the Commonwealths of Virginia and Massachusetts, as well as substantially all material evidence and information, contemporaneously with the service of his Original Complaint.

32. In accordance with the Chicago False Claims Act, Relator will submit an original disclosure statement to the Chicago City Clerk and Chicago Corporation Counsel substantially all material evidence and information, contemporaneously with the service of his Original Complaint.

33. In accordance with the Broward County, Florida and Miami-Dade County, Florida false claims ordinances, Relator will submit an original disclosure to the County Administrator of Broward County, Florida and the County Manager of Miami-Dade County, Florida, as well as substantially all material evidence and information, contemporaneously with the service of his Original Complaint.

V. DEFENDANTS

A. Microsoft

1. Microsoft Corporation

34. Microsoft Corporation is incorporated in the State of Washington and conducts business nationwide. Its principal executive office is located at 1 Microsoft Way, Redmond, Washington 98052-6399. It also maintains a corporate sales office at 11 Times Square, New York, New York 10036. Its registered agent is Corporation Service Company, 80 State Street, Albany, NY 12207-2543.

35. Microsoft Corporation is publicly traded on the New York Stock Exchange under the ticker symbol "MSFT."

36. Microsoft Corporation entered into agreements with the Government Plaintiffs and their agencies related to cloud computing services, licenses, and products, described in further detail *infra*.

2. Microsoft Licensing, G.P.

37. Microsoft Licensing, G.P. is a Nevada general partnership which does business nationwide. Its executive office is located at 6100 Neil Road, Suite 100, Reno, Nevada 89511. Its registered agent is CSC Services of Nevada, Inc., 2215-B Renaissance Drive, Las Vegas, Nevada 89119.

38. Microsoft Licensing, G.P. entered into agreements with some of the Government Plaintiffs and their agencies and subdivisions related to the cloud computing services, licenses, and products at issue, as shown below:

Government Plaintiff	Contracting Subdivision or Agency of Government Plaintiff	Licensed Microsoft Reseller Defendant Affiliated with Associated Sale(s)	Agreement Name	Approximate Agreement Date
State of Florida	Charlotte County	SHI International, Inc.	Enterprise Enrollment	Late 2014
State of Florida	Manatee County	SHI International, Inc.	Enterprise Enrollment	2016
State of Nevada	City of Las Vegas Metropolitan Police Department	SHI International, Inc.	Enterprise Volume Licensing Agreement	August 1, 2016
State of New Mexico	Los Alamos County	SHI International, Inc.	Enterprise Enrollments	July 2014; June 2015

B. Reseller Defendants

39. Microsoft Corporation and Microsoft Licensing, G.P. do not sell products; instead, Microsoft products are sold by licensed resellers. All invoices and price quotes for Microsoft products issued to the Government Plaintiffs were issued by licensed resellers under their letterhead. The following defendants (collectively, "Reseller Defendants") were Microsoft's licensed resellers for the contracts at issue in this case, issued all price quotations and invoices, and entered into contracts with the Government Plaintiffs and their agencies for the sale of Microsoft cloud computing products and services. These contracts are described further *infra*.

40. Pursuant to their contracts with the Government Plaintiffs, the Reseller Defendants listed below often sold additional products and GCC "add-ons" to the Government Plaintiffs, including but not limited to Microsoft's Windows 10 operating system, Microsoft Office 365, and Microsoft's Enterprise Mobility and Security Suite ("EMS").

1. Aerie Consulting, LLC

41. Aerie Consulting, LLC ("Aerie") is a Vermont limited liability company. Its principal executive office is located at 110 West Canal Street, Suite 201, Winooski, Vermont 05404. Its registered agent is Dave Fisher, 110 West Canal Street, Suite 201, Winooski, Vermont 05404.

42. From at least 2016 to the present, Aerie, as a Microsoft licensed reseller, entered into contracts with and sold GCC to the State of Vermont and its local governments, totaling approximately 700 GCC "seats" (users). Pursuant to these contracts, Aerie also sold approximately 365 EMS licenses to the State of Vermont.

2. Alvarez & Associates, LLC

43. Alvarez & Associates, LLC ("Alvarez") is a Virginia limited liability company which does business nationwide. Its principal place of business is 8251 Greensboro Drive, Suite 230, Tysons Corner, Virginia 22102. Its registered agent is Registered Agents, Inc., 4445 Corporation Lane, Suite 264, Virginia Beach, Virginia 23462.

44. From at least 2016 to the present, Alvarez, as a Microsoft licensed reseller, entered into contracts with and sold approximately 46,854 seats of GCC and approximately 6,885 EMS licenses to the Department of Energy, a United States federal government agency. These contracts are described *infra* in further detail.

3. Arctic Information Technology, Inc.

45. Arctic Information Technology, Inc. is an Alaska corporation which does business nationwide. Its principal executive office is at 375 West 36th Avenue, Suite 300, Anchorage, Alaska 99503. Its registered agent is Allen M. Todd, 1 Doyon Place, Suite 300, Fairbanks, Alaska 99701.

46. Arctic Information Technology, Inc. executed contracts with and sold approximately 12,004 seats of GCC and 8,700 EMS licenses to the United States Department of Housing and Urban Development ("HUD") from at least 2015 to the present.

47. Arctic Information Technology, Inc., as a Microsoft licensed reseller, executed contracts with and sold approximately 65,256 seats of GCC and approximately 9,530 EMS licenses to the United States Department of Commerce, a United States federal agency, from at least 2016 to the present.

48. Arctic Information Technology, Inc. executed contracts with and sold over 850 seats of GCC to the United States Department of the Interior from at least 2016 to the present. Pursuant to those contracts, Arctic Information Technology, Inc. also sold EMS to the Department of the Interior.

4. CDW Corporation

49. CDW Corporation ("CDW") is a Delaware corporation which does business nationwide. Its principal executive office is located at 75 Tri-State International, Lincolnshire, Illinois 60069. Its registered agent is Corporation Service Company, 251 Little Falls Drive, Wilmington, Delaware 19808.

50. CDW, as a Microsoft licensed reseller, entered into contracts with the following Government Plaintiffs and their agencies and subdivisions, and sold GCC to those Government Plaintiffs, agencies, or subdivisions from at least 2016 to the present. Pursuant to those contracts, CDW also sold the following Government Plaintiffs additional cloud product offerings as indicated:

Government Plaintiff	Subdivision or Agency	Approx. Seats of GCC Sold	Additional Products Sold Pursuant to Contracts
United States	Broadcasting Board of Governors	1,600	Intune
United States	Department of Energy Headquarters	12,325	EMS
United States	Department of Justice	155	EMS
United States	Department of State	480	Cloud Application Security ("CAS"), EMS, RMS
United States	Government Printing Office	400	EMS
United States	National Aeronautics & Space Administration (NASA)	20	EMS, RMS
State of California	Local Governments	7,732	Intune, EMS, RMS
State of Indiana	County of Hamilton	1,100	EMS
State of Minnesota	Local Governments	3,233	Intune, EMS, RMS
State of Vermont	Department of Buildings & General Services	10,525	EMS
	TOTAL	37,570	

CDW's contracts are described *infra* in further detail.

5. CDW Government, LLC, f/k/a CDW Government, Inc.

51. CDW Government, LLC, formerly known as CDW Government, Inc., is an Illinois limited liability company doing business nationwide. Its principal office is located at 200 North Milwaukee Avenue, Vernon Hills, Illinois 60061. Its registered agent is Corporation Service Company, 801 Adlai Stevenson Drive, Springfield, Illinois 62703.

52. CDW Government, LLC, as a Microsoft licensed reseller, entered into contracts with and sold GCC to the Pension Benefit Guaranty Corporation, a United States federal government agency, from approximately 2012 to 2014.

53. Since 2012, CDW Government, LLC, as a Microsoft licensed reseller, has entered into contracts with and sold approximately 34,222 seats of GCC to the City of Chicago, Illinois, pursuant to a statewide contract with the State of Illinois' Central Management Services.

54. Since October 1, 2015, CDW Government, LLC, as a Microsoft licensed reseller, has entered into contracts with and sold approximately 31,957 seats of GCC to the State of Illinois and its political subdivisions.

55. CDW Government, LLC, as a Microsoft licensed reseller, entered into contracts with the following Government Plaintiffs and their agencies and subdivisions, and sold GCC to those Government Plaintiffs, agencies, or subdivisions from at least 2016 to the present. Pursuant to those contracts, CDW Government, LLC also sold the following Government Plaintiffs additional cloud product offerings as indicated:

Government Plaintiff	**Subdivision or Agency**	**Approx. Seats of GCC Sold**	**Additional Products Sold Pursuant to Contracts**
United States	National Institutes of Health	28,851	Intune, EMS
United States	United States Agency for International Development (USAID)	200	EMS
State of Florida	Lee County	136	AIP
State of Florida	City of Cape Coral	1,182	
State of Florida	City of Gainesville	2,000	
State of Florida	City of Melbourne	870	
State of Illinois	Local Governments	4,293	Intune, EMS, RMS
State of Illinois	Cook County	16,700	EMS
State of Illinois	Dupage County	405	
State of Illinois	Lake County	3,387	
State of Illinois	City of Bloomington	50	
State of Illinois	City of Joliet	451	
State of Illinois	City of Peoria	750	
Commonwealth of Massachusetts	n/a	320	EMS
Commonwealth of Massachusetts	City of Cambridge	1,650	
State of Minnesota	Three Rivers Park District	500	EMS
State of New Jersey	Bergen County	12	
	TOTAL	61,757	

CDW Government, LLC's contracts are described *infra* in further detail.

6. Champion Solutions Group, Inc.

56. Champion Solutions Group, Inc. ("Champion") is a Delaware corporation doing business nationwide. Its principal office is located at 791 Park of Commerce Boulevard, Suite 200, Boca Raton, Florida 33487. Its registered agent is Corporation Service Company, 251 Little Falls Drive, Wilmington, Delaware 19808.

57. Champion, as a Microsoft licensed reseller, entered into a contract with and sold approximately 1,715 seats of GCC to Brevard County, Florida from at least 2016 to the present.

7. CompuCom Systems, Inc.

58. CompuCom Systems, Inc. ("CompuCom") is a Delaware corporation doing business nationwide. Its corporate headquarters are located at 8106 Calvin Hall Road, Fort Mill, South Carolina 29707. Its registered agent is Corporation Service Company, 80 State Street, Albany, NY 12207-2543.

59. Since 2012, CompuCom, as a licensed Microsoft reseller, has entered into contracts with the City of Palo Alto, California and sold it 1,100 seats of GCC.

60. Since 2014, CompuCom, as a Microsoft licensed reseller, has entered into contracts with and sold over 800 seats of GCC (including Office 365) to the Alameda-Contra Costa Transit Authority ("AC Transit").

61. Since 2014, CompuCom, as a Microsoft licensed reseller, has entered into contracts with and sold over 765 seats of GCC to the City of Fairfield, California.

62. Since November of 2014, CompuCom, as a Microsoft licensed reseller, has entered into contracts with and sold approximately 804 seats of GCC to the City of San Mateo, California.

63. Since April of 2015, CompuCom, as a Microsoft licensed reseller, has entered into contracts with and sold approximately 6,179 seats of GCC to the City of Sacramento, California.

64. From at least 2016 to the present, CompuCom, as a Microsoft licensed reseller, entered into contracts with the following subdivisions or agencies of the State of California. Pursuant to these contracts, CompuCom sold the State of California GCC and the additional cloud product offerings indicated below:

Subdivision or Agency of the State of California	**Approx. Seats of GCC Sold**	**Additional Products Sold Pursuant to Contracts**
City of Salinas	750	
City of Santa Monica	1,332	EMS
TOTAL	2,082	

CompuCom's contracts are described *infra* in further detail.

8. Cornerstone IT, Inc.

65. Cornerstone IT, Inc. ("Cornerstone") is an Ohio corporation doing business nationwide. Its principal office is located at 7333 Corporate Boulevard, Mentor, Ohio 44060. Its registered agent is Highland Park Service Corporation, 28601 Chagrin Boulevard, Suite 600, Cleveland, Ohio 44122.

66. Cornerstone entered into a contract with and sold approximately 4,433 seats of GCC to the State of Florida and its local governments from at least 2016 to the present. Pursuant to those contracts, Cornerstone also sold the State of Florida and its local governments RMS and EMS.

9. Crayon Software Experts LLC

67. Crayon Software Experts LLC ("Crayon") is a Delaware limited liability company doing business nationwide. Its principal executive office is located at 12221 Merit

Drive, Suite 800, Dallas, Texas 75251. Its registered agent is the Corporation Trust Company, 1209 Orange Street, Wilmington, Delaware 19801.

68. On or around May 16, 2017, Crayon, as a Microsoft licensed reseller, entered into a contract with and sold approximately 150 seats of GCC to Stanislaus County, California. This contract is described further *infra*.

10. Dell Marketing, L.P.

69. Dell Marketing, L.P. (hereinafter "Dell Marketing") is a Texas limited partnership which does business nationwide. Its principal executive office is located at 1 Dell Way, Round Rock, Texas 78682. Its registered agent is Corporation Service Company, 80 State Street, Albany, NY 12207-2543.

70. From 2012 to the present, Dell Marketing, as a Microsoft licensed reseller, has entered into contracts with and sold over 47,000 seats of GCC to the United States Air Force Air Combat Command, a United States federal government agency.

71. Since June 1, 2012, Dell Marketing, as a Microsoft licensed reseller, has entered into contracts with and sold over 900 seats of GCC to the Delaware River Port Authority, an agency of the State of New Jersey.

72. Dell Marketing, as a Microsoft licensed reseller, entered into a statewide contract with the State of North Carolina in 2014, which expired on June 30, 2017. Pursuant to that contract, Dell Marketing sold GCC to the State of North Carolina and its local governments.

73. Since August 1, 2015, Dell Marketing, as a Microsoft licensed reseller, has entered into contracts with and sold over 815 seats of GCC and over 900 EMS licenses to Camden County, New Jersey.

74. Since at least September 1, 2015, Dell Marketing, as a licensed Microsoft reseller, has entered into contracts with the State of Rhode Island and the Operational Services Division of the Commonwealth of Massachusetts and sold GCC to them. Pursuant to those contracts, Dell Marketing has sold the State of Rhode Island over 8,508 seats of GCC, over 100 Intune licenses, and over 1,286 EMS licenses. Pursuant to those contracts, Dell Marketing has also sold over 4,438 seats of GCC to the Commonwealth of Massachusetts, as well as EMS, AAD, and RMS.

75. Since 2017, Dell Marketing, as a Microsoft licensed reseller, has entered into contracts with and sold over 1,300 seats of GCC and over 1,300 EMS licenses to Middlesex County, New Jersey.

76. Dell Marketing, as a Microsoft licensed reseller, entered into contracts with the following Government Plaintiffs and their agencies and subdivisions, and sold GCC to those Government Plaintiffs, agencies, or subdivisions from at least 2016 to the present. Pursuant to these contracts, Dell Marketing also sold the following Government Plaintiffs the additional cloud product offerings indicated below:

Government Plaintiff	**Subdivision or Agency**	**Approx. Seats of GCC Sold**	**Additional Products Sold Pursuant to Contracts**
United States	U.S. Army	180	
United States	U.S. Coast Guard	560	
United States	Central Intelligence Agency	300	
United States	Department of Defense: Army & Air Force Exchange Services (AAFES)	25	EMS
United States	Department of Education	6,450	
United States	Department of Homeland Security Headquarters	59,000	
United States	Department of Veterans Affairs	12,300	
United States	Federal Emergency Management Agency	29,850	

Government Plaintiff	Subdivision or Agency	Approx. Seats of GCC Sold	Additional Products Sold Pursuant to Contracts
	(FEMA)		
United States	Office of Personnel Management	7,175	
United States	Railroad Retirement Board	378	
United States	Transportation Security Administration (TSA)	100	
District of Columbia	Office of the Chief Technology Officer	300	EMS
State of California	Department of General Services	Over 100,000	
State of California	City of Fresno	10	EMS
State of Indiana	Department of Administration	4,682	EMS
State of Indiana	Local Governments	1,342	EMS, RMS
State of Indiana	City of Indianapolis & Marion County	9,226	
Commonwealth of Massachusetts	City of Worcester	1,500	
State of Montana	Local Governments	36	AIP, EMS, RMS
State of New Jersey	n/a	31,802	EMS
State of New Jersey	Local Governments	2,706	EMS, RMS
State of New Jersey	Essex County	800	
State of New Jersey	Morris County	1,300	EMS
State of North Carolina	Brunswick County	261	EMS
State of North Carolina	City of Fayetteville	1,310	
State of North Carolina	City of Greensboro	150	
State of North Carolina	City of Rocky Mount	1,450	
State of Tennessee	Department of General Services	38,836	EMS, RMS
State of Tennessee	Davidson County and City of Nashville	300	EMS
State of Tennessee	Rutherford County	125	
State of Tennessee	City of Memphis	8,018	
	TOTAL	Over 320,472	

Dell Marketing's contracts are described *infra* in further detail.

11. ECS Federal, LLC

77. ECS Federal, LLC ("ECS") is a Delaware limited liability company doing business nationwide. Its corporate headquarters are located at 2750 Prosperity Avenue, Suite

600, Fairfax, Virginia 22031. Its registered agent is Corporation Service Company, 251 Little Falls Drive, Wilmington, Delaware 19808.

78. Defendant InfoReliance LLC (formerly known as InfoReliance Corporation) has been a wholly-owned subsidiary of ECS since April of 2017.

12. En Pointe Technologies Sales, LLC

79. En Pointe Technologies Sales, LLC ("En Pointe") is a Delaware limited liability company doing business nationwide. Its corporate headquarters are located at 1940 East Mariposa Avenue, El Segundo, California 90245. Its registered agent is the Corporation Trust Company, 1209 Orange Street, Wilmington, Delaware 19081.

80. En Pointe, as a Microsoft licensed reseller, entered into contracts with the following Government Plaintiffs and their agencies and subdivisions, and sold GCC to those Government Plaintiffs, agencies, or subdivisions from at least 2016 to the present. Pursuant to these contracts, En Pointe also sold the following Government Plaintiffs the additional cloud product offerings indicated below:

Government Plaintiff	Subdivision or Agency	Approx. Seats of GCC Sold	Additional Products Sold Pursuant to Contracts
State of California	City and County of San Francisco	45,923	EMS
State of California	City of Oakland	3,827	
State of Hawaii	City and County of Honolulu	2,630	
State of Hawaii	County of Hawaii	1,600	
State of Hawaii	County of Maui	123	
State of Nevada	City of Sparks	745	
State of Rhode Island	Local Governments	223	
	TOTAL	55,071	

81. En Pointe was acquired by Defendant PCM, Inc. in 2015 and became its subsidiary.

13. The Henson Group, Inc.

82. The Henson Group, Inc. ("Henson") is a New York corporation that does business nationwide. Its principal executive office is located at 1375 Broadway, Third Floor, New York, New York 10017-7001. It may be served at The Henson Group, 304 Amboy Avenue, Metuchen, New Jersey 08840.

83. Henson, as a Microsoft licensed reseller, entered into contracts with the State of New Jersey and its local governments, and sold GCC to them from at least 2016 to the present. Pursuant to these contracts, Henson also sold the State of New Jersey and its local governments the additional cloud product offerings indicated below:

Subdivision of the State of New Jersey	Approx. Seats of GCC Sold	Additional Products Sold Pursuant to Contracts
Atlantic County	1,001	EMS
Burlington County	200	
Jersey City	678	
TOTAL	1,879	

14. Imager Software, Inc., d/b/a ISC

84. Imager Software, Inc. (hereinafter "ISC") is a Florida corporation doing business as ISC. Its principal office is located at 2932 Wellington Circle, Tallahassee, Florida 32309. Its registered agent is Brian F. Hearn, 2932 Wellington Circle, Tallahassee, Florida 32309.

85. ISC, as a Microsoft licensed reseller, entered into a contract with and sold approximately 113,875 seats of GCC to the State of Florida and its agencies from at least 2016 to the present. Pursuant to these contracts, ISC also sold RMS and EMS to the State of Florida.

15. InfoReliance LLC, f/k/a InfoReliance Corporation

86. InfoReliance LLC, formerly InfoReliance Corporation ("InfoReliance"), is a Virginia limited liability company which formerly operated as a Virginia corporation. Its principal executive office is located at 2750 Prosperity Avenue, Suite 600, Fairfax, Virginia

22031. Its registered agent is CT Corporation System, 4701 Cox Road, Suite 285, Glen Allen, Virginia 23060.

87. From at least 2014 to the present, InfoReliance, as a Microsoft licensed reseller, entered into contracts with and sold approximately 18,960 seats of GCC to the Department of Labor, a United States federal government agency.

88. From at least 2014 to the present, InfoReliance, as a Microsoft licensed reseller, entered into contracts with and sold approximately 13,863 seats of GCC, over 11,069 EMS licenses, and over 1,800 RMS licenses to the Department of Health and Human Services, a United States federal government agency.

89. InfoReliance was acquired by and is now a wholly-owned subsidiary of Defendant ECS Federal, LLC.

90. InfoReliance's contracts are described *infra* in further detail.

16. Insight Public Sector, Inc., a/k/a Insight Enterprises, Inc.

91. Insight Public Sector, Inc. ("Insight"), also known as Insight Enterprises, Inc., is an Illinois corporation that does business nationwide. Its principal executive office is located at 6820 South Harl Avenue, Tempe, Arizona 85283. Insight also maintains a satellite sales office at 1450 Broadway, 21st Floor, New York, New York 10018. Its registered agent is Corporation Service Company, 80 State Street, Albany, New York 12207-2543.

92. Since 2012, Insight, as a Microsoft licensed reseller, has entered into contracts with Riverside County, California and sold the County approximately 18,125 seats of GCC and over 17,890 EMS licenses.

93. On August 29, 2013, Insight, as a Microsoft licensed reseller, entered into a contract with the United States Postal Service ("USPS"), a United States federal government

agency. To date, Insight has sold approximately 41,726 seats of GCC and approximately 49 EMS licenses to USPS.

94. Since December of 2014, Insight, as a licensed Microsoft reseller, has entered into contracts with and sold approximately 3,892 seats of GCC to Monterey County, California. Pursuant to those contracts, Insight also sold AIP and EMS to Monterey County.

95. Since May 2, 2017, Insight, as a Microsoft licensed reseller, has entered into contracts with and sold GCC to Miami-Dade County, Florida.

96. Since January 1, 2017, Insight, as a Microsoft licensed reseller, entered into contracts with and sold approximately 21,618 seats of GCC to Orange County, California. Pursuant to those contracts, Insight also sold Orange County Intune, EMS, and RMS.

97. Additionally, from at least 2016 to the present, Insight, as a Microsoft licensed reseller, entered into contracts with the following Government Plaintiffs and their agencies and subdivisions, and sold GCC to those Government Plaintiffs, agencies, or subdivisions. Pursuant to those contracts, Insight also sold the following Government Plaintiffs additional cloud product offerings as indicated:

Government Plaintiff	**Subdivision or Agency**	**Approx. Seats of GCC Sold**	**Additional Products Sold Pursuant to Contracts**
United States	Environmental Protection Agency	63,040	EMS
United States	Federal Reserve System	4,419	EMS
United States	Department of the Navy	727	EMS
State of California	City of Orange	800	
State of Iowa	n/a	630	Intune, AIP, EMS, RMS
State of Iowa	Polk County	5	
State of Iowa	City of Cedar Rapids	35	
State of Iowa	City of Des Moines	473	
State of Iowa	City of West Des Moines	590	
Commonwealth of Virginia	Fairfax County	15,270	EMS

Government Plaintiff	Subdivision or Agency	Approx. Seats of GCC Sold	Additional Products Sold Pursuant to Contracts
	TOTAL	85,989	

Insight's contracts are described *infra* in further detail.

17. Intraprise TechKnowlogies LLC

98. Intraprise TechKnowlogies LLC ("Intraprise") is a Hawaii limited liability company. Its principal office is located at 1110 Nuuanu Avenue #18, Honolulu, Hawaii 96817. Its registered agent is Donny Shimamoto, 178 Walker Avenue, Wahiawa, Hawaii 96786.

99. Intraprise, as a Microsoft licensed reseller, entered into contracts with and sold over 700 seats of GCC to the State of Hawaii and its agencies and local governments from at least 2016 to the present.

18. Liftoff, LLC

100. Liftoff, LLC ("Liftoff") is a Delaware corporation that does business nationwide. Its corporate headquarters are located at 2138 Priest Bridge Court, Suite 120, Crofton, Maryland 21114. Its registered agent is Registered Agent Solutions, Inc., 9 East Loockerman Street, Suite 311, Dover, Delaware 19901.

101. From at least 2016 to the present, Liftoff, as a Microsoft licensed reseller, entered into contracts with and sold: (1) over 920 seats of GCC to the State of Tennessee and its local governments; and (2) over 1,703 seats of GCC to the Commonwealth of Virginia and its local governments. Liftoff also sold approximately 32 EMS licenses to the State of Tennessee and approximately 250 EMS licenses to the Commonwealth of Virginia and its local governments.

19. Lilien, LLC, a/k/a Lilien Systems

102. Lilien, LLC ("Lilien"), also known as Lilien Systems, is a Delaware limited liability company which does business nationwide. Its principal executive office is located at 17

East Sir Francis Drake Boulevard, Suite 110, Larkspur, California 94939-1708. Its registered agent is National Registered Agents, Inc., 160 Greentree Drive, Suite 101, Dover, Delaware 19904.

103. From at least 2016 to the present, Lilien, as a Microsoft licensed reseller, entered into contracts with and sold approximately 545 seats of GCC to Sacramento County, California.

104. Lilien is a subsidiary of Sysorex Government Services, Inc., a Virginia corporation.

20. Minburn Technology Group LLC

105. Minburn Technology Group LLC ("Minburn") is a Virginia limited liability company that does business nationwide. Its principal executive office is located at 10113 Minburn Street, Great Falls, Virginia 22066. Its registered agent is Anthony John Colangelo, 10113 Minburn Street, Great Falls, Virginia 22066.

106. From at least 2016 to the present, Minburn, as a Microsoft licensed reseller, entered into contracts with and sold GCC to the following Government Plaintiffs:

Government Plaintiff	**Subdivision or Agency**	**Approx. Seats of GCC Sold**
United States	Department of the Treasury	150
United States	Internal Revenue Service	186,000
United States	Securities and Exchange Commission (SEC)	6,000
United States	Small Business Administration	3,500
United States	Special Operations Command	4,000
	TOTAL	199,650

Minburn's contracts are described *infra* in further detail.

21. PCM, Inc.

107. PCM, Inc. is a Delaware corporation doing business nationwide. Its corporate headquarters are located at 1940 East Mariposa Avenue, El Segundo, California 90245. It also

maintains a satellite sales office at 1 Penn Plaza, 36th Floor, New York, New York 10119. Its registered agent is CT Corporation System, 28 Liberty Street, New York, New York 10005.

108. PCM, Inc. is publicly traded on the New York Stock Exchange under the ticker symbol "PCM."

109. Defendants En Pointe Technologies Sales, LLC and PCMG, Inc. are subsidiaries of PCM, Inc.

22. PCMG, Inc. d/b/a PCM Gov, Inc.

110. PCMG, Inc. ("PCMG") is a Delaware corporation that does business nationwide as PCM Gov, Inc. Its corporate headquarters are located at 13755 Sunrise Valley Drive, Suite 750, Herndon, Virginia 20171. Its registered agent is CT Corporation System, 28 Liberty Street, New York, NY 10005.

111. Beginning in September of 2015, PCMG, as a Microsoft licensed reseller, entered into contracts with and sold approximately 108,936 seats of GCC and over 23,371 EMS licenses to the City and County of Los Angeles, California, pursuant to a contract with the Los Angeles County Community Development Commission. These contracts were paid with United States federal funds provided by the U.S. Department of Housing and Urban Development.

112. From at least 2016 to the present, PCMG, as a Microsoft licensed reseller, entered into contracts with the States of California and Minnesota and their local governments, and sold GCC to them, as shown below. Pursuant to those contracts, PCMG also sold the following Government Plaintiffs additional cloud product offerings as indicated:

Government Plaintiff	Subdivision or Agency	Approx. Seats of GCC Sold	Additional Products Sold Pursuant to Contracts
State of California	Fresno County	30	
State of California	San Mateo County	6,022	EMS
State of California	Tuolumne County	642	

Government Plaintiff	Subdivision or Agency	Approx. Seats of GCC Sold	Additional Products Sold Pursuant to Contracts
State of California	City of Roseville	1,100	
State of California	City of San Jose	9,195	
State of Minnesota	Washington County	35	EMS
State of North Carolina	City of Winston-Salem	130	
	TOTAL	17,154	

PCMG's contracts are described *infra* in further detail.

113. PCMG is a subsidiary of Defendant PCM, Inc.

23. Planet Technologies, Inc.

114. Planet Technologies, Inc. ("Planet") is a Delaware corporation that does business nationwide. Its corporate headquarters are located at 20400 Observation Drive, Suite 107, Germantown, Maryland 20876. It also maintains a satellite sales office in New York City. Its registered agent is CT Corporation System, 28 Liberty Street, New York, New York 10005.

115. From at least 2016 to the present, Planet, as a Microsoft licensed reseller, entered into contracts with the following Government Plaintiffs and their agencies and subdivisions, and sold GCC to those Government Plaintiffs, agencies, or subdivisions. Pursuant to those contracts, Planet also sold the following Government Plaintiffs additional cloud product offerings as indicated:

Government Plaintiff	Subdivision or Agency	Approx. Seats of GCC Sold	Additional Products Sold Pursuant to Contracts
United States	Department of Defense: Defense Commissary Agency (DeCA)	200	
State of California	State Government Operations	3,343	
State of California	Madera County	50	
State of California	San Joaquin County	297	
State of Florida	City of Clearwater	100	
State of Florida	City of Daytona Beach	4	
State of New Jersey	Cape May County	650	

Government Plaintiff	Subdivision or Agency	Approx. Seats of GCC Sold	Additional Products Sold Pursuant to Contracts
State of North Carolina	Buncombe County	1,690	
State of North Carolina	Orange County	157	
State of North Carolina	Surry County	655	
State of North Carolina	City of Greenville	530	EMS
	TOTAL	7,676	

Planet's contracts are described *infra* in further detail.

24. Procentrix, Inc.

116. Procentrix, Inc. ("Procentrix") is a Virginia corporation. Its corporate headquarters are located at 2201 Cooperative Way, Suite 550, Herndon, Virginia 20171. Its registered agent is CT Corporation System, 4701 Cox Road, Suite 285, Glen Allen, Virginia 23060.

117. From at least 2016 to the present, Procentrix, as a Microsoft licensed reseller, entered into contracts with and sold approximately 901 seats of GCC to the United States Courts, a division of the United States federal government.

25. ProSum Inc., a/k/a ProSum Technologies

118. ProSum Inc. ("ProSum"), also known as ProSum Technologies, is a California corporation. Its principal executive office is located at 2201 Park Place, Suite 102, El Segundo, California 90245. Its registered agent is Ravi Prem Chatwani, 2201 Park Place, Suite 102, El Segundo, California 90245.

119. From at least 2016 to the present, ProSum, as a Microsoft licensed reseller, entered into contracts with and sold approximately 1,035 seats of GCC to Kern County, California.

26. SHI International Corporation, f/k/a Software House International, Inc.

120. SHI International Corporation ("SHI"), formerly known as Software House International, Inc., is a New Jersey corporation doing business nationwide. Its corporate headquarters are located at 290 Davidson Avenue, Somerset, New Jersey 08873. It also maintains a satellite sales office at One Penn Plaza, Suite 2705, New York, New York 10119. Its registered agent is CT Corporation System, 28 Liberty Street, New York, New York 10005.

121. From 2012 to the present, SHI, as a Microsoft licensed reseller, has entered into contracts with and sold over 4,857 seats of GCC to the Commonwealth of Virginia (through the Virginia Information Technology Agency, an agency of the Commonwealth), and approximately 325 seats of GCC to Loudoun County, Virginia. Pursuant to those contracts, SHI also sold over 270 EMS licenses to Loudoun County and over 4,884 EMS licenses to the Commonwealth of Virginia.

122. From 2012 to the present, SHI, as a Microsoft licensed reseller, has entered into contracts with and sold over 62,145 seats of GCC to the State of North Carolina. Pursuant to those contracts, SHI has also sold EMS to the State of North Carolina.

123. From 2013 to the present, SHI, as a Microsoft licensed reseller, has entered into contracts with and sold over 249 seats of GCC to Indian River County, Florida.

124. From September 16, 2013 to the present, SHI, as a Microsoft licensed reseller, has entered into contracts with and sold over 430 seats of GCC to the State of Delaware and its local governments. Pursuant to these contracts, SHI also sold the State of Delaware EMS.

125. From at least 2014 to the present, SHI entered into contracts with and sold approximately 2,652 seats of GCC to the City of St. Petersburg, Florida.

126. Since April 1, 2015, SHI has entered into contracts with and sold approximately 2,310 seats of GCC to the Pension Benefit Guaranty Corporation, a United States federal agency.

127. Since June of 2015, SHI has entered into contracts with and sold over 750 seats of GCC and EMS to Los Alamos County, New Mexico.

128. From at least 2015 to the present, SHI entered into contracts with and sold GCC to the State of Minnesota's Department of Information Technology Services.

129. From at least 2015 to the present, SHI entered into contracts with and sold GCC to the Florida Housing Finance Corporation, a Florida state agency.

130. From at least 2015 to the present, SHI entered into contracts with and sold approximately 3,300 seats of GCC and over 250 EMS licenses to Pinellas County, Florida.

131. From at least 2016 to the present, SHI, as a Microsoft licensed reseller, entered into contracts with the following Government Plaintiffs and their agencies and subdivisions, and sold GCC to those Government Plaintiffs, agencies, or subdivisions. Pursuant to those contracts, SHI also sold the following Government Plaintiffs additional cloud product offerings as indicated:

Government Plaintiff	**Subdivision or Agency**	**Approx. Seats of GCC Sold**	**Additional Products Sold Pursuant to Contracts**
United States	Bureau of Indian Affairs	80	Intune, EMS
United States	Federal Commissions Boards Councils	8,186	Intune, EMS
State of Delaware	City of Wilmington	1,025	EMS
State of Florida	South Florida Water Management District	1,800	EMS
State of Florida	Southwest Florida Water Management District	600	EMS
State of Florida	Broward Health	3,678	
State of Florida	Broward County	5,825	Intune, EMS
State of Florida	Charlotte County	2,009	EMS
State of Florida	Collier County	376	
State of Florida	Hillsborough County	7,035	EMS

Government Plaintiff	Subdivision or Agency	Approx. Seats of GCC Sold	Additional Products Sold Pursuant to Contracts
State of Florida	Lake County	1,040	EMS
State of Florida	Manatee County	1,800	
State of Florida	Marion County	1,035	
State of Florida	Miami-Dade County	19,028	EMS
State of Florida	Orange County	525	EMS
State of Florida	Osceola County	1	EMS
State of Florida	Palm Beach County	445	
State of Florida	Pasco County	1,557	
State of Florida	Sarasota County	182	
State of Florida	Seminole County	1,300	
State of Florida	St. Johns County	165	EMS
State of Florida	City of Coral Springs	100	
State of Florida	City of Fort Myers	976	
State of Florida	City of Jacksonville and Duval County	475	
State of Florida	Town of Jupiter	Unknown	
State of Florida	City of Miami	2,900	EMS
State of Florida	City of Miramar	1,000	
State of Florida	City of Ocala	705	EMS
State of Florida	City of Pensacola	750	
State of Florida	City of Port St. Lucie	370	
State of Florida	City of Tampa	200	EMS
Commonwealth of Massachusetts	Barnstable County	300	EMS, RMS
State of Minnesota	Anoka County	2,176	
State of Minnesota	Blue Earth County	488	
State of Minnesota	Ramsey County	700	
State of Minnesota	Scott County	860	EMS
State of Minnesota	Sherburne County	7	
State of Minnesota	City of Minneapolis	5,252	EMS
State of Minnesota	Metropolitan Area of Minneapolis	10	
State of Minnesota	City of Rochester	25	
State of Minnesota	City of St. Paul	5,650	
State of Montana	n/a	6,111	RMS
State of Nevada	City of Henderson	1,580	EMS
State of Nevada	City of Las Vegas	450	EMS
State of New Mexico	General Services Department	5,718	EMS
State of New Mexico	Local Governments	605	EMS
State of New Mexico	Bernalillo County	661	EMS, Intune
State of New Mexico	City of Albuquerque	65	EMS, Intune
State of North	Local Governments	4,927	AIP, EMS

Government Plaintiff	Subdivision or Agency	Approx. Seats of GCC Sold	Additional Products Sold Pursuant to Contracts
Carolina			
State of North Carolina	Durham County	200	
State of North Carolina	City of High Point	1,400	EMS
State of Virginia	Henrico County	4,241	
State of Virginia	City of Charlottesville	700	
State of Virginia	City of Lynchburg	1,278	
State of Virginia	City of Norfolk	7,792	EMS
State of Virginia	City of Portsmouth	1,750	
State of Virginia	City of Richmond	3,800	EMS
State of Virginia	City of Virginia Beach	4,486	
	TOTAL	126,400	

SHI's contracts are described *infra* in further detail.

27. Softchoice Corporation

132. Softchoice Corporation ("Softchoice") is a New York corporation that does business nationwide. The headquarters for Softchoice's government contracting division is 7800 Westpark Drive, Suite T400, McLean, Virginia 22102. Softchoice maintains a satellite sales office at 50 Broad Street, Suite 701, New York, New York 10004. Its registered agent is National Registered Agents Inc., 28 Liberty Street, New York, New York 10005.

133. From at least 2013 to the present, Softchoice, as a Microsoft licensed reseller, executed contracts with and sold over 100 seats of GCC and over 180 EMS licenses to the Farm Credit Administration, a United States federal agency.

134. From at least 2016 to the present, Softchoice, as a Microsoft licensed reseller, executed contracts with and sold over 2,800 seats of GCC to the Federal Communications Commission ("FCC"), a United States federal agency. Pursuant to these contracts, Softchoice also sold RMS to the FCC.

135. From at least 2016 to the present, Softchoice, as a Microsoft licensed reseller, executed contracts with and sold approximately 4,296 seats of GCC and approximately 550 EMS licenses to the Federal Small Independent Agencies, a division of the United States federal government.

136. Softchoice's contracts are discussed *infra* in further detail.

28. Software One, Inc.

137. Software One, Inc. is a Wisconsin corporation doing business nationwide. Its principal executive office is located at 20875 Crossroads Circle, Suite 1, Waukesha, Wisconsin 53186. It maintains a satellite sales office at 401 Park Avenue South, 10th Floor, New York, New York 10016. Its registered agent is CT Corporation System, 301 South Bedford Street, Suite 1, Madison, Wisconsin 53703.

138. Since 2012, Software One, Inc., as a licensed Microsoft reseller, has entered into contracts with San Bernardino County, California and sold it approximately 3,800 seats of GCC and 600 EMS licenses.

139. Since 2015, Software One, Inc., as a licensed Microsoft reseller, entered into contracts with and sold approximately 18,169 seats of GCC and over 5,465 EMS licenses to San Diego County, California.

140. From at least 2016 to the present, Software One, Inc., as a licensed Microsoft reseller, entered into contracts with the following Government Plaintiffs and sold them GCC. Pursuant to those contracts, Software One, Inc. also sold the following Government Plaintiffs additional cloud product offerings as indicated:

Government Plaintiff	Subdivision or Agency	Approx. Seats of GCC Sold	Additional Products Sold Pursuant to Contracts
United States	Federal Deposit Insurance	9,300	EMS

Government Plaintiff	Subdivision or Agency	Approx. Seats of GCC Sold	Additional Products Sold Pursuant to Contracts
	Corporation		
State of California	Department of Justice and Public Safety	250	EMS
State of California	Health and Human Services Agency	860	Intune, EMS
State of California	East Bay Regional Park District	845	
State of California	Alameda County	9,701	
State of California	Contra Costa County	1,550	EMS
State of California	Marin County	150	EMS
State of California	San Luis Obispo County	2,700	
State of California	Santa Cruz County	929	
State of California	Shasta County	858	
State of California	Solano County	3,694	
State of California	Sonoma County	50	
State of California	Ventura County	10,050	EMS, RMS
State of California	City of Anaheim	2,100	
State of California	City of Irvine	1,134	
State of California	City of Long Beach	4,277	EMS
State of California	City of Pasadena	175	EMS
State of California	City of San Diego	8,279	
State of California	City of Santa Clara	1,045	
State of California	City of Stockton	1,600	
State of California	City of Sunnyvale	200	
State of California	City of Vallejo	450	
State of North Carolina	Mecklenburg County	6,565	EMS
State of North Carolina	City of Charlotte	300	EMS
	TOTAL	67,062	

Software One, Inc.'s contracts are described *infra* in further detail.

29. Solid Networks Inc.

141. Solid Networks Inc. is a California corporation headquartered at 5686 Pirrone Road, Salida, California 95368. Its registered agent is Joseph Edward Cram, 5686 Pirrone Road, Salida, California 95368.

142. From at least 2016 to the present, Solid Networks Inc., as a licensed Microsoft reseller, entered into contracts with and sold approximately 4,500 seats of GCC to the State of California. Pursuant to these contracts, Solid Networks Inc. also sold the State of California over 22,310 EMS licenses.

30. Sysorex Government Services, Inc.

143. Sysorex Government Services, Inc. is a Virginia corporation headquartered at 13880 Dulles Corner Lane, Suite 175, Herndon, Virginia 20171. Its registered agent is National Registered Agents, Inc., 4701 Cox Road, Suite 285, Glen Allen, Virginia 23060.

144. Defendant Lilien, LLC, also known as Lilien Systems, is a subsidiary of Sysorex Government Services, Inc.

31. T4 Technologies, Inc.

145. T4 Technologies, Inc. is a Minnesota corporation. Its principal executive office is located at 3322 Stinson Boulevard Northeast, Minneapolis, Minnesota 55418. Its registered agent is Robert J. Scott, 3322 Stinson Boulevard Northeast, Minneapolis, Minnesota 55418.

146. From at least 2015 to the present, T4 Technologies, Inc., as a Microsoft licensed reseller, entered into contracts with and sold approximately 35,018 seats of GCC to the State of Minnesota. Pursuant to those contracts, T4 Technologies, Inc. also sold approximately 33,980 EMS licenses to the State of Minnesota.

32. Ventech Solutions Inc.

147. Ventech Solutions Inc. ("Ventech") is a Delaware corporation that does business nationwide. Its principal executive office is located at 8425 Pulsar Place, Suite 300, Columbus, Ohio 43240. Its registered agent is The Corporation Trust Company, 1209 Orange Street, Wilmington, Delaware 19801.

148. From at least 2016 to the present, Ventech, as a licensed Microsoft reseller, entered into contracts with the Centers for Medicare and Medicaid Services ("CMS"), a United States federal government agency. Pursuant to these contracts, Ventech sold CMS approximately 10,000 seats of GCC.

VI. RESPONDEAT SUPERIOR AND VICARIOUS LIABILITY

149. Any and all acts alleged herein to have been committed by the Defendants were committed by officers, directors, employees, representatives, or agents, who at all times acted on behalf of the Defendants and within the course and scope of their employment, or by corporate predecessors to whom successor liability applies.

150. Defendants Microsoft Corporation and Microsoft Licensing, G.P. (collectively "Microsoft") are related entities sharing common employees, offices, and business names such that they are jointly and severally liable under legal theories of respondeat superior.

151. Defendants CDW Corporation and CDW Government, LLC (formerly known as CDW Government, Inc.) are related entities sharing common employees, offices, and business names such that they are jointly and severally liable under legal theories of respondeat superior.

152. Defendants ECS Federal, LLC and InfoReliance LLC are related entities sharing common employees, offices, and business names such that they are jointly and severally liable under legal theories of respondeat superior.

153. Defendants En Pointe Technologies Sales, LLC, PCMG, Inc., and PCM, Inc. are related entities sharing common employees, offices, and business names such that they are jointly and severally liable under legal theories of respondeat superior.

154. Defendants Lilien, LLC and Sysorex Government Services, Inc. are related entities sharing common employees, offices, and business names such that they are jointly and severally liable under legal theories of respondeat superior.

VII. BACKGROUND

A. Cloud Computing

155. Cloud computing provides software, data storage and hosting, services, networks, and applications over the Internet. It enables "ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources . . . that can be rapidly provisioned and released with minimal management effort or service provider interaction." Ex. 3, NIST Special Publication 800-145 (2011), at 6.

156. There are three types of cloud computing service models: Software as a Service ("SaaS"), Platform as a Service ("PaaS"), and Infrastructure as a Service ("IaaS"). *See* Ex. 3, NIST Special Publication 800-145, at 6–7. SaaS allows a customer to use the cloud provider's applications in a cloud infrastructure. Ex. 3, NIST Special Publication 800-145, at 6. PaaS allows customers to deploy their own applications utilizing program languages, services, and tools from the cloud provider. Ex. 3, NIST Special Publication 800-145, at 6–7. IaaS provides customers with "fundamental computing resources" such as processing, storage, and networks so that the customers can run their own operating systems, applications, or other arbitrary software. Ex. 3, NIST Special Publication 800-145, at 7.

157. No matter which service model is utilized, cloud services are provided via one of four types of deployment models: private cloud, community cloud, public cloud, or hybrid cloud. Private cloud services are provisioned for use by one organization. Ex. 3, NIST Special Publication 800-145, at 7. Community cloud services are provisioned for use by a specified

community of consumers "from organizations that have shared concerns (e.g., mission security requirements, policy, and compliance considerations)." *Id.* Public cloud services are provisioned for use by the general public. *Id.* Hybrid cloud services are a combination of private, community, or public cloud deployment models. *Id.* For example, under this hybrid deployment model, sensitive data could be stored in a private cloud while less sensitive data and operations are in a public cloud.[3]

158. When a state, local, or federal government entity seeks a cloud services provider, it must make sure that sensitive government data will be protected. To do this, state and local entities will typically consult security standards propagated by the FBI's Criminal Justice Information Services Division ("CJIS"). Federal entities, in contrast, will examine standards and certifications issued by the Federal Risk and Authorization Management Program ("FedRAMP").

159. While the CJIS standards provide technical information regarding the assessment of different security issues and a framework for doing so, they do not explicitly set a preference or requirement for one type of deployment model over another, leaving such determinations up to the individual government entity.

160. Some cloud providers sign "CJIS agreements" with states, which assure that the signatory has procedures and systems in place for safeguarding criminal justice information and screening personnel with access to that information. These agreements, unlike the CJIS standards, do set out requirements which the signatory provider must comply with. To date, Microsoft has signed CJIS agreements covering Microsoft Azure and Office 365 with thirty-four

[3] Some Microsoft marketing materials refer to "hybrid" deployment models as those which combine physical infrastructure with cloud services. This is not the same definition of "hybrid cloud" utilized by the National Institute of Standards and Technology ("NIST") and elsewhere in this document.

states, including the Government Plaintiff states of California, Florida, Hawaii, Illinois, Indiana, Iowa, Minnesota, Montana, New Jersey, Nevada, North Carolina, Rhode Island, Tennessee, and Vermont, as well as the Commonwealths of Massachusetts and Virginia.[4]

161. FedRAMP is a United States government-wide program which allows federal agencies to adopt cloud solutions more quickly and easily, providing a "marketplace" of products which have already gained FedRAMP accreditation at the "low", "moderate", or "high" security levels.[5] Federal agencies can assess their security needs with FedRAMP tools, and choose providers that allegedly meet those needs on the FedRAMP online marketplace.

162. A cloud provider's FedRAMP certification does not preclude the possibility of fraud related to the security of the cloud offering—it only means that the provider has passed the certification test. FedRAMP certification tests also do not examine whether the cloud product offered actually conforms to its marketing or contractual promises. FedRAMP certification also does not reflect compliance with state standards or CJIS agreements.

163. GCC, the cloud product primarily at issue in this case, was certified "FedRAMP Moderate" during the period at issue.

164. Some state, local, or federal government entities have their own cloud frameworks for assessment of cloud providers, which set out specific requirements rather than a set of guidelines for evaluation. Others specifically bar certain cloud deployment models. For example, the United States Postal Service specifically bars processing or storing sensitive

[4] *See* Microsoft, *Criminal Justice Information Services (CJIS) Security Policy* (July 1, 2018), https://www.microsoft.com/en-us/trustcenter/Compliance/CJIS

[5] Referred to as "FedRAMP Low", "FedRAMP Moderate", and "FedRAMP High".

information in a public cloud. United States Postal Service, Information Security Handbook AS-805 § 3-5.3 (Dec. 2018).[6]

165. Services or data stored within a public cloud, rather than a community or private cloud, are more vulnerable to breach. According to CJIS, when cloud services "reside within a shared infrastructure[,] . . . [t]his increases the risk of data spillage across logical (customer) boundaries either by intentional manipulation . . . or unintentional spillage due to administrator error . . . or data manipulation operations." Ex. 5, CJIS Recommendations for Implementation of Cloud Computing Solutions (Aug. 10, 2012), at 3. For this reason, many government agencies prefer to utilize a "government community cloud" deployment model, in which the infrastructure is only shared by governments and certain trusted government service providers bound by government security or compliance standards.

B. Microsoft Cloud Products & Services

166. Microsoft does not sell products or cloud services directly to government customers. Instead, it sells through authorized resellers such as the Reseller Defendants. The reseller enters into contracts with customers, and Microsoft enters into "agreements" with those same customers—including licensing agreements and business agreements. The licensed reseller also issues all price quotations and invoices to customers under its letterhead.

167. Microsoft provides over 200 cloud services, which are hosted in Microsoft's cloud infrastructure. The most prominent cloud services at issue in this case are discussed in more detail below.

168. Microsoft has provided cloud services "for government," which purport to offer segregated cloud services to a specified community of government users, since 2012.

[6] *Available at* http://about.usps.com/handbooks/as805/as805c3_013.htm

1. Microsoft Azure

169. Microsoft Azure ("Azure") is a cloud service which provides all three service models of cloud computing: SaaS, PaaS, and IaaS. The services at issue in this matter mainly fall within the SaaS and PaaS service models.

170. Azure's default deployment model for businesses in the United States is the "Azure commercial cloud," a public cloud that is generally geographically limited to the United States with regard to customers, data storage, and management.

171. Microsoft also offers "Azure Government", a cloud service that purportedly has a government community cloud deployment model. Microsoft allegedly only offers Azure Government to federal, state, local, and tribal government entities and their partners. The iteration of Azure Government at issue in this case is called "GCC," and, as explained *infra*, was not a true "government community cloud."

172. Azure Government utilizes the Azure Active Directory ("AAD") as a "keyring" to manage users' identities—usernames and passwords. AAD also manages user permissions—what services, products, and data users can access. GCC's iteration of AAD operates in the Azure commercial cloud, rather than a government-only community cloud. AAD comes in two varieties: AAD Basic, which is the default for GCC, and AAD Premium, which is a more expensive "upgrade" to AAD Basic.

173. Beginning in 2017, Microsoft began to offer two government community cloud services that are more private and secure, and are specifically for the U.S. Department of Defense and certain other federal agencies, defense contractors, and the intelligence community. These products are referred to internally as "Azure Trailblazer," "Azure Government DoD," "Azure Government Defense," "Azure Government High," or "Azure PathFinder." These

services operate under a true government community cloud framework and are not at issue in this case.

2. Enterprise Mobility & Security Suite ("EMS")

174. EMS is a bundle, or "suite" of products and services offered by Microsoft alongside its cloud services. It includes products such as Intune, AIP, and CAS that provide identity protection, security, file encryption, device and application management, and mobile device management.

175. Azure Information Protection ("AIP") classifies and then encrypts files so that if the files are stolen or viewed by the wrong person, they will be unreadable. A user must log in to the Azure network and be given the proper permissions in order to view files encrypted by AIP. AIP is a product developed by Secure Islands. AIP utilizes a Microsoft technology called Rights Management System ("RMS") to encrypt files and documents. When utilized with GCC, this implementation of AIP with RMS operates entirely in the Azure commercial cloud, including the encryption keys themselves.

176. Cloud Application Security ("CAS") is a product developed by Israeli company Adallom, which was acquired by Microsoft in September of 2015. CAS is given credentials to log into an organization's various cloud services. It looks for sensitive files and data that should not be located within certain parts of the cloud. If CAS finds such files and data, it will show the user where they are located, log the location, and save related information. CAS helps track who has files and where the files are. CAS also operates and stores data in the Azure commercial cloud.

177. During Relator's employment, Microsoft had future plans to integrate CAS with AIP, so that sensitive files located by CAS in the "wrong hands" could be automatically encrypted by AIP.

178. EMS automatically includes AIP and CAS, but those two products must be activated in order for a customer to use them.

179. Microsoft Intune ("Intune") is a device management tool that enables organizations to apply application, data, and device management controls across iOS, Windows, Android, and MacOS devices. Intune appeared in and was operated from the "government console" for GCC users, but this was purely cosmetic—the GCC iteration of Intune operates and stores information entirely within the Azure commercial cloud.

3. Microsoft Office 365

180. Microsoft Office 365 is a monthly SaaS subscription service that provides software—including Microsoft Word, Outlook, PowerPoint, OneNote, and Excel—alongside online collaboration capabilities, file hosting, and other associated services.

181. Microsoft offers several iterations of Office 365, including "Office 365 for U.S. Government." Office 365 for U.S. Government purportedly utilizes a government community cloud deployment model.

182. The GCC iteration of Office 365 for U.S. Government at issue in this case utilizes commercial AAD for management of user credentials, passwords, and user permissions.[7]

[7] In 2018, Microsoft introduced "Microsoft Office 365 GCC High", which appears to be a true government community cloud version of Office 365—unlike GCC's iteration of Office 365, which partially utilizes the commercial cloud. Microsoft Office 365 GCC High was not provided to any of the Government Plaintiffs and is not at issue in this case.

4. Microsoft Cloud Product "Suites"

183. Microsoft's product "suites" for government customers come in three different varieties—G1, G3, and G5, from least to most expensive.

184. Until fairly recently, Microsoft also sold "Enterprise" plans to government customers—designated as E1 for Government, E3 for Government, and E5 for Government. The E1, E3, and E5 plans "for Government" have features similar to the G1, G3, and G5 plans. Today, Microsoft still offers Office 365 Enterprise E1, E3, and E5 plans, but does not advertise them as "for Government." However, some government entities are "grandfathered" in to using E1, E3, or E5 plans when renewing existing contracts and agreements with Defendants.

185. All of the above product suites, as well as all iterations of GCC, utilize AAD to manage sign-ins and user identities.

C. Contracts

186. The following chart sets out the contracts at issue in this matter currently known to Relator. Statewide contracts are denoted by the addition of an asterisk (*) after the name of the Government Plaintiff. All municipality and agency contracts entered into pursuant to those statewide contracts are bound by their certifications, terms, and conditions.

187. Defendants' alleged violations of the False Claims Act, and state and local False Claims Acts, concern more contracts than those listed below. The Reseller Defendants entered into additional contracts, the details of which are unknown to Relator, to make the sales of GCC and other cloud products and services described *supra* in Section V(B).

Government Plaintiff	Agency or Subdivision of Gov't Plaintiff	Reseller Defendant	Effective Date(s)	Contract Number(s) or Identifier(s), if Known	Contract Amount or Value, if Known	Exhibit No., if Applicable
United States	Department of Energy	Alvarez	11/18/16–4/29/19	DE-IM0000759	$55,056.65	

Government Plaintiff	Agency or Subdivision of Gov't Plaintiff	Reseller Defendant	Effective Date(s)	Contract Number(s) or Identifier(s), if Known	Contract Amount or Value, if Known	Exhibit No., if Applicable
United States	Department of Health & Human Services	Info-Reliance; ECS Federal	11/20/14–9/23/19	Award ID HHSP23337002	$8,623,504.73	
United States	Department of State	CDW Corp.	9/12/16–9/13/18	Award ID SAQMMA16L1049	$5,000	
United States	Department of State	CDW Corp.	3/10/17–5/31/17	Award ID SAQMMMA17L0344	$163,020	
United States	Department of the Treasury	Minburn	7/6/17–6/19/18	Award No. TIRNO17T00043	$285,514.10	
United States	Farm Credit Administration	Softchoice	9/14/13–9/30/16	13-FCA-601-064	$540,527.48	
United States	Farm Credit Administration	Minburn	12/27/16–present	17-FCA-651-016		
United States	FCC	Softchoice	7/13/15–present	Award ID FCC15G0079	$7,529.28	
United States	Internal Revenue Service	Minburn	6/20/17–6/19/20	Award ID TIRNO17T00043	$254,123.09	
United States	Pension Benefit Guaranty Corporation	SHI	4/1/15–3/31/18	GS-35F-0111K	$5,149,432.91	Ex. 2
United States	Pension Benefit Guaranty Corporation	CDW Government, LLC	9/30/11–9/30/14	GS-35F-0195J	$1,166,450.63	Ex. 4
United States	Small Business Administration	Dell Marketing	1/22/16–1/21/20	GS-35F-059DA	$11,000	
United States	USAID	CDW Government, LLC	9/12/16–9/13/18	Award ID SAQMMA16L1049	$5,000	

Government Plaintiff	Agency or Subdivision of Gov't Plaintiff	Reseller Defendant	Effective Date(s)	Contract Number(s) or Identifier(s), if Known	Contract Amount or Value, if Known	Exhibit No., if Applicable
United States	United States Postal Service	Insight Public Sector	8/29/13–8/28/19	1BITSW-13-B-0016	$1,190,884.44	
United States	United States Postal Service	Insight Public Sector	8/29/13–8/28/19	1BITSW-16-C-0098	$9,303.12	
District of Columbia	Office of the Chief Technology Officer	Dell Marketing	12/1/16–11/30/19	CW47643	$10,000,000[8]	
State of California*	Department of General Services	Dell Marketing	6/15/17–6/14/20	1-17-70-50B		Ex. 12
State of California	AC Transit	Compu-Com	Feb. 2014–present	RIVCO-20800-007-12/14	$1,434,464.80	
State of California/ United States (federally funded contract)	Los Angeles County Community Development Commission	PCMG	9/1/15–8/31/20	RIVCO-20800-005-12/12	$1,198,079.90	Ex. 14
State of California	Monterey County	Insight Public Sector	7/1/14–6/30/17		$57,600	
State of California	Orange County	Insight Public Sector	1/1/17–10/31/19	MA-017-17011185, under Riverside County contract		Ex. 34

[8] Maximum value of contract, of which $2,914,334.47 had been paid as of October 10, 2018.

Government Plaintiff	Agency or Subdivision of Gov't Plaintiff	Reseller Defendant	Effective Date(s)	Contract Number(s) or Identifier(s), if Known	Contract Amount or Value, if Known	Exhibit No., if Applicable
State of California	Riverside County[9]	CompuCom; Dell Marketing; En Pointe; Insight Public Sector; PCMG; SoftChoice	11/1/16–10/31/19	RIVCO-20800-003; RIVCO-20800-005	$24,000,000	
State of California	Stanislaus County	Crayon Software Experts LLC	5/16/17–5/16/20		$1,900,000	Ex. 37
State of California	City of Fairfield	CompuCom	2014–present			
State of California	City of Irvine	Software One	2016–present		$3,800,000	
State of California	City of Palo Alto	CompuCom	2012–present	C12144913	$275,363	
State of California	City of Pasadena	Software One	4/1/16–3/31/19		$1,500,000	
State of California	City of Sacramento	CompuCom	4/16/15–4/16/20		$3,520,000	
State of California	City of San Diego	Software One	2015–present		$1,870,436.59	
State of California	City of San Jose	PCMG			$359,258	
State of California	City of San Mateo	CompuCom	2012–2/13/18	EA #7800891	$540,220	
State of California	City of Vallejo	Software One	2016–present		$450,000	
State of Delaware*	Local Governments	SHI	12/15/16–present	NASPO # ADSPO16-130651		Ex. 38
State of Delaware	City of Wilmington	SHI	9/17/18–9/17/21		$905,945.22	

[9] Plus other counties and local governments (shared contract).

Government Plaintiff	Agency or Subdivision of Gov't Plaintiff	Reseller Defendant	Effective Date(s)	Contract Number(s) or Identifier(s), if Known	Contract Amount or Value, if Known	Exhibit No., if Applicable
State of Florida*	Department of Management Services	SHI	1/29/16–present	43230000-15-2		Ex. 39
State of Florida	Florida Housing Finance Corp.	SHI	2015–present		$83,663.57	
State of Florida	Broward County	SHI	10/31/17–11/1/20	A2115141G1_1	$5,985,414[10]	
State of Florida	Charlotte County	SHI	9/23/14–present	Under statewide contract 252-001-09-1	$279,775.42	
State of Florida	Jacksonville-Duval County	SHI	5/6/16–5/5/19	Bid No. XC-0483-16	$2,767,411.27	
State of Florida	Lee County	SHI	10/1/16–1/31/19	Under statewide contract 43230000-15-2		
State of Florida	Lee County	SHI	8/21/18–4/7/20			
State of Florida	Manatee County	SHI	2016–present	Under statewide contract 252-001-09-1	$1,050,000	
State of Florida	Marion County	SHI	2016–present	12C-066	$265,947.85	
State of Florida	Miami-Dade County	SHI	4/22/16–5/31/17	Under statewide contract 43230000-15-2	$7,955,000	
State of Florida	Miami-Dade County	Insight Public Sector	5/31/17–5/2/20	FB-00472	$28,600,000	
State of Florida	Miami-Dade County	SHI	4/8/16–4/7/19	NASPO # ADSPO16-130651		Ex. 38

[10] Total contract amount, of which $3,484,732.74 had been paid as of April 22, 2019.

Government Plaintiff	Agency or Subdivision of Gov't Plaintiff	Reseller Defendant	Effective Date(s)	Contract Number(s) or Identifier(s), if Known	Contract Amount or Value, if Known	Exhibit No., if Applicable
State of Florida	Nassau County	SHI	12/1/17–11/30/18[11]	Under statewide contract 43230000-15-2	$51,159.86	
State of Florida	Pinellas County	SHI	6/30/15–9/30/21	145-0364-S(RG)	$3,776,997.40	Ex. 40
State of Florida	City of Clearwater	Planet			$1,670,000	
State of Florida	City of Jupiter	SHI	11/3/16–11/3/19	Under statewide contract 43230000-15-2	$536,661	
State of Florida	City of Miramar	SHI	7/17/15–7/1/21	Under statewide contract 43230000-15-2	$1,072,000	Ex. 41
State of Florida	City of Port St. Lucie	SHI	2/1/16–1/31/19	20170033, under statewide contract 43230000-15-2	$353,000	
State of Florida	City of St. Petersburg	SHI	2/1/14–1/31/17		$119,421.85	
State of Florida	City of St. Petersburg	SHI	2/1/17–1/31/18		$314,929.28	
State of Florida	City of St. Petersburg	SHI	2/1/18–2/1/21	Under statewide contract 43230000-15-2	$2,154,509.91	
State of Illinois*	Central Management Services	CDW Government, LLC	10/1/11–9/30/15	CMS2595580		Ex. 42
State of Illinois	City of Bloomington	CDW Government, LLC			$176,166.17	Ex. 43

[11] Upon information and belief, this contract's expiration date was extended upon its expiration.

Government Plaintiff	Agency or Subdivision of Gov't Plaintiff	Reseller Defendant	Effective Date(s)	Contract Number(s) or Identifier(s), if Known	Contract Amount or Value, if Known	Exhibit No., if Applicable
State of Illinois	City of Chicago Department of Innovation & Technology	CDW Government, LLC	5/25/12–9/30/15	26250, under statewide contract CMS2595580	$6,000,000	Ex. 42
State of Indiana*	Department of Administration	Dell Marketing	6/26/02–9/30/21	53AAJ		
State of Iowa*	n/a	Insight Public Sector	5/1/16–4/30/21	4400006644		Ex. 44
Commonwealth of Massachusetts*	n/a	CDW Government, LLC	3/1/16–3/31/20	30882		
Commonwealth of Massachusetts*	Operational Services Division	CDW Government, LLC	4/11/16–present	ITS58		
Commonwealth of Massachusetts*	Operational Services Division	Dell Marketing	6/29/15–6/30/20	ITS58		
State of Minnesota*	Office of MN.IT Services	SHI	2015–present	6089180		
State of Minnesota	City of Eden Prairie	SHI	2016–present		$115,690.84	
State of Minnesota	City of Rochester	SHI	2016–present	Under statewide contract 6089180	$550,000	
State of Montana*	n/a	SHI	4/8/16–4/7/19	NASPO # ADSPO16-130651		Ex. 38

Government Plaintiff	Agency or Subdivision of Gov't Plaintiff	Reseller Defendant	Effective Date(s)	Contract Number(s) or Identifier(s), if Known	Contract Amount or Value, if Known	Exhibit No., if Applicable
State of Nevada*	n/a	SHI	4/8/16–4/7/19	NASPO # ADSPO16-130651		Ex. 38
State of Nevada	City of Henderson[12]	SHI	10/1/16–4/8/19	NASPO # ADSPO16-130651		Ex. 38
State of Nevada	City of Las Vegas Metropolitan Police Department	SHI	8/1/16–7/31/19		$1,255,936	
State of New Jersey*	n/a	Dell Marketing	6/30/16–6/30/20	89850		
State of New Jersey	Delaware River Port Authority	Dell Marketing	6/1/12–5/31/18	Under statewide contract A77003	$922,692.27	
State of New Jersey	Camden County	Dell Marketing	8/1/15–3/31/17	9900186334	$100,665	
State of New Jersey	Camden County	Dell Marketing	3/31/17–present	Under statewide contract 89850	$75,000	
State of New Jersey	Middlesex County	Dell Marketing	6/30/17–6/30/20	Under statewide contract 89850	$415,443.48	
State of New Mexico*	General Services Department	SHI	4/8/16–4/7/19	NASPO # ADSPO16-130651		Ex. 38
State of New Mexico	Bernalillo County	SHI	2016–present		$1,880,106.50	
State of New Mexico	Los Alamos County	SHI	7/8/14–7/8/17[13]	AGR15-4126	$443,284.56	Ex. 45
State of New Mexico	City of Albuquerque	SHI	3/27/18–3/21/20	SHR00021432	$112,710.81	
State of North Carolina*	n/a	SHI	5/11/10–4/30/20	ITS-400175		

[12] Under a Nevada statewide contract.
[13] Upon information and belief, this contract's expiration date was extended upon its expiration.

Government Plaintiff	Agency or Subdivision of Gov't Plaintiff	Reseller Defendant	Effective Date(s)	Contract Number(s) or Identifier(s), if Known	Contract Amount or Value, if Known	Exhibit No., if Applicable
State of North Carolina*	n/a	SHI	3/1/14–2/28/19	400251		
State of North Carolina	City of High Point	SHI	4/8/16–4/7/19	NASPO # ADSPO16-130651		Ex. 38
State of Rhode Island*	Division of Purchases	Dell Marketing	9/1/15–6/30/20	ITS58	$250,000	
State of Tennessee*	Department of General Services	Dell Marketing	4/1/15–3/31/20	SWC No. 3006		Ex. 46
State of Tennessee	City of Memphis	Dell Marketing	6/24/15–6/23/19	32392	$557,216	Ex. 46
Commonwealth of Virginia*	Virginia Information Technology Agency ("VITA")	SHI	10/7/10–10/7/13	VA-070907-SHI		Ex. 47
Commonwealth of Virginia*	VITA	SHI	10/7/13–present	VA-131017-SHI		Ex. 48
Commonwealth of Virginia	Fairfax County	Insight	5/1/16–4/30/21	4400006644		Ex. 44
Commonwealth of Virginia	Loudoun County	SHI	6/15/11–6/16/14	Under VA statewide contract VA-070907-SHI	$2,200,000	
Commonwealth of Virginia	Loudoun County	SHI	7/16/14–7/16/17	Under VA statewide contract VA-131017-SHI	$1,421,185	
State of Vermont*	Dep't of Buildings & General Services	CDW Corp.	3/1/16–present	Addendum No. 30649		
State of Vermont*	Dep't of Buildings & General Services	CDW Corp.	3/1/16–3/31/20	30882		

Government Plaintiff	Agency or Subdivision of Gov't Plaintiff	Reseller Defen-dant	Effec-tive Date(s)	Contract Number(s) or Identifier(s), if Known	Contract Amount or Value, if Known	Exhibit No., if Appli-cable
				TOTAL	**Over $142,789,701**	

188. The Reseller Defendants issued all price quotations and invoices associated with the above contracts.

D. Certifications

189. Defendants made the following certifications in their contracts and agreements with the Government Plaintiffs.

1. Compliance with Applicable Laws

190. Defendants certified their compliance with applicable laws, rules, and regulations in the contracts at issue.

191. For example, Defendant SHI's contract ADSPO-16-130651 with the State of Delaware, Miami-Dade County, the State of Montana, the State of Nevada, the State of New Mexico, and the State of North Carolina contains the following certification: "18. Laws and Regulations[:] Any and all products offered and furnished shall comply with solicitation section 5.10, Compliance with Applicable Laws." Ex. 38, NASPO Multistate Contract, at 29. The appropriate section of the lead state's solicitation[14] states: "The materials and services supplied under this Contract shall comply with all applicable Federal, state and local laws, and the Contractor shall maintain all applicable license and permit requirements." Ex. 38, NASPO Multistate Contract, at 56.

[14] Section 5.10 of the solicitation from the lead state addresses another issue, so the reference appears to be mis-numbered. The quoted solicitation language is from the appropriate section, which bears a different paragraph number.

192. The following contracts and agreements between the Government Plaintiffs and Defendants also include certifications as to compliance with applicable laws, rules, and/or regulations.

Government Plaintiff	Contracting Agency or Division of Government Plaintiff	Date of Contract or Agreement	Agreement Name or Contract Number	Defendant Signatory to Contract or Agreement	Exhibit Number and Page(s)
United States	Pension Benefit Guaranty Corporation	9/30/2011	GS-35F-0195J	CDW Government, LLC	Ex. 4, at 12
United States	Pension Benefit Guaranty Corporation	4/1/2015	GS-35F-0111K	SHI	Ex. 2, at 30
State of California	Department of General Services	6/15/2017	1-17-70-50B (and all contracts entered into under it)	Dell Marketing, L.P.	Ex. 12, p. 6
State of California	Department of General Services	6/15/2017	1-17-70-50B: Online Services Terms (and all contracts entered into under it)	Dell Marketing, L.P. & Microsoft	Ex. 12, p. 67
State of California	Los Angeles County Community Development Commission	8/28/2015	Enterprise Enrollment Amendment	Microsoft Corp.	Ex. 49, p. 26
State of California	Los Angeles County Community Development Commission	9/3/2015	RIVCO-20800-005-12/12	PCMG	Ex. 14, p. 13
State of California	Los Angeles County Community Development Commission	5/23/2016	RIVCO-20800-005-12/12	PCMG	Ex. 50, p. 14
State of California	Orange County	1/1/2017	MA-017-17011185	Insight Public Sector	Ex. 34, p. 10

Government Plaintiff	Contracting Agency or Division of Government Plaintiff	Date of Contract or Agreement	Agreement Name or Contract Number	Defendant Signatory to Contract or Agreement	Exhibit Number and Page(s)
State of California	San Bernardino County	6/28/2011	Terms and Conditions	Software One, Inc.	Ex. 51, p. 2
State of Florida	Department of Management Services	1/29/2016	43230000-15-02 and all contracts entered into under it	SHI	Ex. 39, p. 5
State of Florida	Department of Management Services	3/14/2016	State and Local Enterprise Agreement (for all purchases under statewide contract 43230000-15-02)	Microsoft Corp.	Ex. 52, p. 20
State of Illinois	Central Management Services	2018	CMS2595580 (and all contracts entered into under it)		Ex. 42, p. 29
State of Illinois	City of Chicago Department of Innovation & Technology	5/25/2012	26250	CDW Government, LLC	Ex. 42, pp. 17, 30
State of Tennessee	Department of General Services	6/24/2015	SWC No. 3006 (and all contracts entered into under it)	Dell Marketing	Ex. 46, p. 24

193. Similarly, the State of Iowa's statewide Master Agreement with Defendant Insight Public Sector, effective May 1, 2016 to April 30, 2019, includes the following compliance certification: "Contractor agrees . . . All work and services [are] rendered in strict conformance to all laws, statutes, and ordinances and the applicable rules, regulations, methods and procedures of all government boards, bureaus, offices and other agents." Ex. 44, Iowa Statewide

& Fairfax County, Virginia Contract, at 55. This contract is shared between the State of Iowa and Fairfax County, Virginia.

194. Defendant SHI, in its October 4, 2007 statewide contract VA-070907-SHI with the Commonwealth of Virginia, certified the following: "Contractor agrees to comply with all provisions of the then current security procedures of VITA and the appropriate Authorized User(s) as are pertinent to Contractor's operation and have been supplied to Contractor by VITA and the Authorized User(s) and further agrees to comply with all applicable federal, state and local laws." Ex. 47, Virginia Statewide Contract VA-070907-SHI, at 17. Virginia's follow-up contract with SHI from 2013 contains a nearly-identical certification. *See* Ex. 48, Virginia Statewide Contract VA-131017-SHI, at 18–19.

195. Defendants made similar representations in other contracts, currently unknown to Relator, under which the sales described in Section V(B) *supra* took place.

2. Conformity with Representations

196. In Illinois statewide contract CMS2595580, Defendant CDW Government, LLC certified that "supplies furnished under [the] contract" would "conform to the standards, specifications, drawing, samples or descriptions furnished by the State or furnished by the Vendor and agreed to by the State." Ex. 43, Bloomington & Illinois Statewide Contract, at 30. This certification is binding on all contracts entered into under statewide contract CMS2595580.

197. Defendants made similar representations in other contracts, currently unknown to Relator, under which the sales described in Section V(B) *supra* took place.

VIII. DEFENDANTS' FRAUD ON THE GOVERNMENT

198. Defendants have fraudulently caused the Government Plaintiffs to pay hundreds of millions of dollars for cloud computing services that operate partially within the public

"commercial cloud" while representing to the Government Plaintiffs that those products and services operate securely within an exclusive "government cloud." These "fake" government cloud services put government data at an increased risk of breach.

199. In particular, Defendants: (1) fraudulently induced the Government Plaintiffs and their agencies to enter into contracts and agreements and purchase "fake" government cloud services via false or misleading marketing; (2) made false statements in their contracts and agreements with the Government Plaintiffs; and (3) made false certifications in their contracts and agreements with the Government Plaintiffs.

A. Defendants fraudulently induced the Government Plaintiffs to enter into contracts based on false information about the cloud services at issue.

200. Microsoft advertises cloud services "for Government" that purportedly operate entirely within a cloud that is exclusive to U.S. government agencies, and are segregated from non-government users.[15] In reality, Microsoft offers two different kinds of services "for government." The first is a "true" government cloud service targeted at the U.S. Department of Defense and other high-security government agencies (often referred to internally as "Azure Government High," "Trailblazer," "PathFinder," "Azure Defense," or "Azure Government DoD.") The second, however, is a "fake" government cloud. This second service—at issue in the instant case—is typically referred to as "GCC" or "Government Community Cloud."[16] It stores user identities and many crucial security functions in the general "commercial cloud" that Microsoft offers to all commercial consumers in the United States, while falsely displaying that it is operating in a government cloud.

[15] *E.g.*, https://enterprise.microsoft.com/en-us/trends/the-microsoft-cloud-for-government/ (last accessed Mar. 29, 2019).

[16] The product called "Azure Government" officially became available to government customers on December 9, 2015. However, GCC, operating partially in the commercial cloud, has been available to government customers since 2012 in one form or another. .

201. Despite this key difference, no public Microsoft marketing materials or representations to the Government Plaintiffs during the time period at issue adequately identified that the GCC cloud services at issue—including the GCC versions of Azure Government, Office 365, and EMS—were services that ran or stored data partially in the commercial cloud.

202. In fact, Microsoft marketing materials, websites, and PowerPoint presentations targeted towards government customers have made the following false representations about the exclusivity and characteristics of Microsoft's "government cloud" services—including GCC—as far back as 2012 and continuing to the present day:

- "Microsoft Azure Government delivers a *physical and network-isolated instance* of Azure, including most of the hyper-scalable IaaS and PaaS services that Azure offers and the security and compliance standards needed for Public Sector."[17] Ex. 35, Azure Government Slide with Speaker Notes (2012), at 1.

- "Azure Government is a government-community cloud (GCC)[.] . . . The Azure Government environment *is a completely separate instance from Microsoft Azure public* and *only used* by qualified U.S. government organizations and solution providers. . . . Identity Management within the Azure Government environment is a separate instance of Azure Active Directory." Ex. 6, Microsoft Azure Government Overview (Dec. 2014), at 3–4 (emphasis added).

- "Identity Management within the Azure Government environment *is a separate instance* of Azure Active Directory." Ex. 6, Microsoft Azure Government Overview, at 5 (emphasis added).

- "Public Sector entities receive *a physically isolated instance* of Microsoft Azure that employs world-class security and compliance services critical to U.S. government *for all systems and applications built on its architecture*." Ex. 7, Microsoft Azure Government Information Sheet (2016), at 1 (emphasis added).

- "The most trusted cloud for mission-critical government workloads . . . A *physically isolated instance* of Microsoft Azure, built *exclusively for government customers* and their solution providers." Ex. 7, Microsoft Azure Government Information Sheet (2016), at 1 (emphasis added).

[17] The "slide script" accompanying this PowerPoint slide further states: "These datacenters [for Microsoft Azure Government] are physically isolated from Azure commercial services[.]" Ex. 35, at 1.

- "The Azure Government cloud *is dedicated to* our United States based government customers." Ex. 8, Microsoft Azure Government PowerPoint (June 29, 2016), at 3 (emphasis added).

- "Your [government] organization's customer content[18] *is logically segregated from* customer content in Microsoft's commercial Office 365 services." Ex. 9, Office 365 US Government Service Description (Feb. 14, 2017), at 1 (emphasis added).

- "The Microsoft Government Cloud provides screened personnel, *physical isolation*, and commitments to public sector compliance." Ex. 67, Microsoft CJIS Implementation Guidelines (July 2016), at 3 (emphasis added).

- "Microsoft has made a commitment to U.S. Public Sector by providing cloud solutions *that can only be utilized by U.S. government entities* and/or customers subject to government compliance regulations." Ex. 67, Microsoft CJIS Implementation Guidelines, at 9 (emphasis added).

- "Secure and compliant cloud for US government only . . . Physically separated instance of Microsoft Azure." Ex. 10, Ignite PowerPoint (Sept. 2017), at 2.

- "Your data is segregated from commercial data[.]" Ex. 11, Office 365 Government Plans Description (Oct. 16, 2017), at 3.

- Office 365 for Government plans "provide all the features and capabilities of Office 365 services *in a segmented government cloud community*[.]"[19]

- "Only US federal, state, local and tribal governments and their partners have access to this *dedicated instance* that only screened U.S. citizens operate."[20]

- "Azure Government is a government-only cloud you can trust, *exclusively for US federal, state, local, and tribal government agencies* and their partners. A physical and logical *network-isolated instance* of Microsoft Azure . . . specifically designed to meet the needs of US government agencies and their partners." Ex. 13, Microsoft Azure Government Contact Form, at 1 (emphasis added).

In truth, GCC is neither government-exclusive nor separated completely from commercial data, because it partially utilizes the general commercial cloud. Microsoft's misrepresentations in this regard continue to this day.

[18] Including identities (usernames and passwords).
[19] https://products.office.com/en-us/government/compare-office-365-government-plans (last accessed Mar. 29, 2019) (emphasis added).
[20] https://azure.microsoft.com/en-us/overview/clouds/government/ (last accessed Mar. 29, 2019) (emphasis added).

203. The following components or products ran or stored data either partially or completely within the commercial cloud: AAD, RMS, AIP, CAS, and Intune. Microsoft, however, marketed and licensed these products and components to government customers without revealing that the products operated within the commercial cloud. *See, e.g.*, Ex. 9, Office 365 US Government Service Description, at 9–10 (noting that RMS and AAD are available in a government community cloud without mentioning commercial cloud overlap). In fact, one Microsoft document even falsely states that a separate instance of AAD ran "within the Azure Government environment." Ex. 6, Microsoft Azure Government Overview, at 5. In truth, a "true" separate government cloud version of AAD could not be used with GCC at all.

204. GCC's partial use of the commercial cloud, rather than a true segregated government cloud, makes government data more vulnerable to breach and hacking. *See, e.g.*, Ex. 5, CJIS Recommendations for Implementation of Cloud Computing Solutions (Aug. 10, 2012), at 3, 7. Placement of user identities in the commercial cloud through AAD presents a particularly high risk of breach because user identities are used to log in to GCC and view secured or encrypted data and documents. Identities are typically a hacker's first target, as they secure and allow access to other parts of a network.

205. Furthermore, the Government Plaintiffs use GCC for confidential and highly sensitive government documents and data, including but not limited to police body camera footage, court records, criminal justice information, and healthcare records.

206. Microsoft sold GCC to government customers with a "fake SKU."[21] This SKU, or product identification code, actually sold the customer Microsoft's regular commercial cloud product alongside its partial government community cloud. Microsoft planned to eventually

[21] Microsoft employees even used the term "fake SKU" internally.

migrate the commercial cloud components of GCC into an actual government community cloud framework, but did not divulge to government customers that GCC was not yet a true government community cloud. Microsoft utilized the "fake SKU" so that it would not have to execute new agreements or sales contracts once it implemented a "true" government community cloud for GCC customers—which never occurred during Relator's employment with Microsoft. *See* Ex. 53, E-mail Chain between Relator, Phil West, and Others (Oct. 21–25, 2016), at 2.

207. Once a government customer contracted for and began using GCC, the deception continued. The government agency's users would see a "government portal" whenever they logged in to Azure, perpetuating the myth that everything within Azure took place within a segregated "government cloud."[22] However, in reality, if those users were to log in to Azure's commercial portal with their government cloud username and password, they would discover that their identities—and many Azure cloud functions—were actually in the commercial cloud.

208. Microsoft also falsely claimed that the entirety of Microsoft Azure (which includes GCC) was "FedRAMP High" certified. *See* Microsoft, Government Cybersecurity Imperative, Washington Post (May 8, 2016).[23] During the time period at issue, GCC was only "FedRAMP Moderate" certified—a lower level of security.

209. Similarly, Microsoft signed CJIS agreements with many of the Government Plaintiff states, and claimed that GCC and its services were compliant with those agreements. *See, e.g.*, Ex. 9, Office 365 US Government Service Descriptions, at 1. However, the Azure commercial cloud was not compliant with the CJIS agreements, rendering GCC noncompliant via its partial use of the commercial cloud.

---

[22] Identities which showed up in the "government portal" were not even government cloud copies—they were in the commercial cloud.

[23] *Available at* https://www.washingtonpost.com/sf/brand-connect/microsoft/wp/enterprise/government-cybersecurity-imperative-a-microsoft-perspective/?noredirect=on

210. While some *internal* Microsoft documents reveal that GCC partially operated and stored some data in the commercial cloud, the marketing material referenced above does not state this, and government customers were unaware of this fact. An August 2016 internal PowerPoint presentation illustrates an intent to eventually migrate all GCC services to an exclusive government cloud. However, GCC was marketed and sold to government customers *long before* this migration occurred. In fact, the migration never occurred during Relator's employment with Microsoft Corporation.[24]

211. Only in October of 2017—after the majority of the contracts at issue were signed—did *any* public Microsoft website reveal that any of the GCC cloud services at issue operated in the Azure commercial cloud. For example, on October 20, 2017, Microsoft published an article on its Microsoft Azure informational page entitled "Planning Identity for Azure Government Applications." *See* Ellis & Saca, *Planning Identity for Azure Government Applications*, MICROSOFT AZURE (Oct. 20, 2017).[25] This article reveals that Office 365 for GCC and its AAD component operates within the commercial cloud, distinguishing them from the "true" government cloud. *Id.* However, this article is buried within Microsoft Azure's informational webpages. Furthermore, Defendants made no alterations to their contracts and agreements with the Government Plaintiffs or other GCC marketing materials following publication of the article.

212. Defendants entered into procurement contracts and agreements with the Government Plaintiffs and their agencies and subdivisions, as previously outlined. Defendants procured the contracts via fraudulent conduct, including: (1) false marketing and advertising,

[24] Relator also learned from another Microsoft employee that such a migration would be nearly impossible to perform.

[25] *Available at* https://docs.microsoft.com/en-us/azure/azure-government/documentation-government-plan-identity

such as that outlined above; (2) false representations and communications to the Government Plaintiffs regarding GCC's cloud deployment model; and (3) false statements about the cloud services provided within the contracts and agreements themselves.

213. GCC's partial usage of the commercial cloud was acknowledged within Microsoft as an ongoing problem, as shown by a January 24, 2017 "OneList" issue tracker page accessible company-wide. *See* Ex. 54, GCC OneList Issue Tracker (Sept. 16, 2015), at 1. The OneList page reads, in relevant part:

> --When will O365 GCC customers expect to have their [A]AD tenant provisioned in Azure Government [A]AD?
> --When will existing O365 GCC customers have their tenants moved into the Azure Government AD environment?
> Impact: Selling EMS/ECS/[EMS] G5 to GCC customers is not possible. It is impacting nationwide (USA) SLG/Federal accounts requiring GCC.

Ex. 54, at 1. Although the document notes that selling EMS to GCC customers "is not possible" as a result of GCC's instance of AAD and EMS not residing in a true government cloud, Microsoft ignored this issue. *Id.* Defendants encouraged sales of and actually sold EMS and GCC to hundreds of governments and government agencies, including the Government Plaintiffs.

214. Furthermore, despite Relator's many efforts to stop Microsoft's deceptive marketing to government customers, Defendants took no action to inform the Government Plaintiffs that the GCC services at issue were running and storing data partially in the commercial cloud, placing secure government data at risk and perpetuating deception of the Government Plaintiffs.

215. In fact, Microsoft concealed GCC's security flaws, specifically instructing Relator and others not to demonstrate AIP to GCC customers. The AIP demonstration process at the time would alert a GCC customer to the fact that their identities were in the commercial cloud

(rather than a government cloud), because it required logging into the commercial Azure console. Microsoft told Relator and others to simply not do this, so that it could keep the Government Plaintiffs ignorant.

216. To provide another example of Microsoft's fraudulent practices, AAD operates with all services within GCC, managing user "identities" and log-ins using the commercial cloud. This is one of the most security-crucial functions in a cloud environment, because those same identities can allow a hacker to access data everywhere that log-in allows access to. Microsoft continuously marketed and/or provided GCC to the Government Plaintiffs since 2012 as an exclusive government community cloud service, notwithstanding the fact that AAD operates in the commercial cloud. Microsoft has therefore marketed or provided "fake" government cloud services to the Government Plaintiffs and their agencies and subdivisions. Additionally, Microsoft continues to offer EMS and GCC to government customers to this day,[26] notwithstanding the fact that components of both operate within the commercial cloud.

217. Virtually all of the contracts and agreements between Defendants and the Government Plaintiffs in this case contain no indication or reference to the fact that GCC operated partially within the government cloud, as explained further below.

218. Even the contracts which do make this disclosure do not tell the whole truth. For example, Exhibit 4 to Appendix A to the June 15, 2017 statewide contract (contract # 1-17-70-50B) between Dell Marketing and the State of California's Department of General Services discloses that some GCC operations occur within the Azure commercial cloud:

> For clarity, as of the effective date of [this] Government Contract, certain Microsoft Azure Plans (and License Suite Plans) that contain "public cloud"

[26] *See* Julia White, *Government IT Modernization Reaches Tipping Point*, MICROSOFT (Mar. 5, 2018), *available at* https://cloudblogs.microsoft.com/industry-blog/government/2018/03/05/government-it-modernization-reaches-tipping-point/ (last accessed Mar. 29, 2019).

> versions of Microsoft Azure Services . . . may be purchased under the [State of California's] Enterprise Agreement for the purpose of managing or enhancing one or more other Microsoft Online Services. Examples include, but are not limited to, SKUs for the Microsoft Enterprise Mobility and Security suite ("EMS"). . . . For clarity, Microsoft:
> 1. Does not represent such public cloud version of Azure Services . . . as "FedRAMP High" (they have FedRAMP Moderate ATO);
> 2. Does not represent such services to be "Azure Government Services" for sale under the Government Contract. . . .
> [S]ome same-named Services . . . may be available for the State [of California] to consume for other purposes under the Government Contract as Azure Government Services. Such services may include, but not be limited to, Azure Active Directory Premium.

Ex. 12, California Statewide Dell Contract, at 37–38. In particular, the contract notes that Azure Active Directory "may be available for the State to consume . . . *as Azure Government Services*." Ex. 12, California Statewide Dell Contract, at 38. However, AAD was *not* a "government service" in the GCC iteration sold to the State of California—it partially operated in the commercial cloud. In other words, while California's statewide contract alerted users that EMS partially used the public cloud, as shown above, it did not do so with regard to AAD or GCC as a whole. And, it only indicated the *possibility* of acquiring commercial AAD, rather than alerting the customer that GCC was actually using commercial AAD.

219. To provide another example, a March 3, 2015 Volume Licensing Agreement Enterprise Enrollment Amendment entered into between Microsoft Corporation and the State of Minnesota's information technology department—part of Minnesota's statewide contract 6089180 with SHI International—states:

> "Community" means the community consisting of one or more of the following: (1) a Government, (2) an Enrolled Affiliate using Azure Government Services to provide solutions to a Government or a qualified member of the Community, or (3) an Enrolled Affiliate with Customer Data that is subject to Government regulations for which the Enrolled Affiliate determines the use of Azure Government Services, and not Windows Azure Services, is the appropriate Microsoft service to meet the Enrolled Affiliate's regulatory requirements. . . .
> **EMS for Government Terms** . . .

> **c. Windows Intune.** Government Partner understands and acknowledges that Windows Intune, the third individual component of the EMS-G Suite, will not be provisioned in multi-tenant data centers for exclusive use by or for the Community.
> **d. [AAD Premium] for Government and Azure RMS for Government.** Government Partner understands and acknowledges that AADP-G [AAD Premium for Government] and RMS-G [RMS for Government] will not initially be provided in multi-tenant data centers for exclusive use by or for the Community. However, AADP-G and RMS-G will be provisioned in multi-tenant data centers for exclusive use by or for the Community at a future date. As soon as practicable following such future date, the AADP-G and RMS-G services Government Partner is acquiring on behalf of Enrolled Affiliate will be migrated to the Community multi-tenant data centers.

Ex. 55, Minnesota Enrollment Agreements (March 3, 2015), at 18–19 (emphasis in original). AAD and RMS were never migrated into a "true" government-exclusive cloud during Relator's employment at Microsoft. Thus, even though the excerpt above concedes that EMS's iterations of AAD Premium, RMS, and Intune are not "exclusive" to government users (due to their use of the commercial cloud in part), it still makes a false statement with regard to Microsoft's plans to migrate users into a "true" government cloud. Furthermore, the agreement does not explain that the lack of exclusivity is due to GCC's partial use of the commercial (public) cloud. It also restricts itself to EMS and AAD Premium, rather than discussing how the problem impacted AAD Basic and GCC as a whole.

220. Microsoft and Microsoft Licensing's Indirect Enterprise Enrollment Agreement with some local governments—including Manatee County, Florida—contain a similar "partial" disclosure. These agreements state that Office 365 for Government is offered in a government community cloud, but then acknowledge that "Other Office 365-branded or separately branded Online Services that may be made available as part of or in addition to Office 365 for Government are not included in the Government Community Cloud." Ex. 56, Manatee County Agreements, at 18. This is only a partial disclosure of the truth. GCC's iteration of Office 365

for Government is not truly offered in a government community cloud, because it uses commercial AAD to manage identities. Further, the agreement does not specify which "Online Services" are not included in the Government Community Cloud. The disclosure also restricts its discussion to Office 365, rather than disclosing how this issue impacted GCC as a whole.

221. While Microsoft, SHI, and Dell Marketing partially revealed the truth to a few select Government Plaintiffs, Defendants concealed GCC's commercial cloud operations from the other Government Plaintiffs by not including parallel provisions in all contracts and agreements. This shows that Defendants knowingly defrauded the Government Plaintiffs.

222. Additionally, Microsoft was well aware of how to craft an agreement informing government customers of the fact that a particular product operated in the commercial cloud. In fact, Microsoft did so with regard to the product "Yammer." GCC customers who wished to purchase Yammer executed an amendment to their enterprise enrollment agreement with Microsoft which stated, in relevant part:

> Yammer Enterprise *is provided in a "public cloud," not in a "community cloud,"* as such terms are defined in NIST Special Publication 800-145. *It is neither part of, nor a component of, Office 365 for Government*.
> In the event that Microsoft integrates Yammer Enterprise features or functionality into any Office 365 for Government Online Service, Microsoft makes no representation or warranty that Enrolled Affiliate will be able to migrate its Customer Data from Yammer Enterprise to Office 365 for Government, nor that any such migration (if possible) will be performed by Microsoft at no cost.

Ex. 57, City of Sparks Enterprise Enrollments, at 15 (emphasis added). This shows that Microsoft knowingly stated falsely that its other GCC services—including those which utilized the commercial cloud—were in a government-exclusive community cloud.

223. The Government Plaintiffs would not have entered into the contracts and agreements at issue or paid claims under those contracts had they known that they were not obtaining "true" government cloud services, but "fake" government cloud services that ran and

stored data partially in the commercial cloud. *See, e.g.*, Ex. 50, 2016 Los Angeles County Contract, at 27 (Statement of Work specifying that PCMG shall provide "Azure *for Government*") (emphasis added); United States Postal Service, Information Security Handbook AS-805 § 3-5.3 (Dec. 2018)[27] (prohibiting storing or processing sensitive information in a public cloud).

B. Defendants made false statements in their contracts and agreements with the Government Plaintiffs.

224. Defendants' contracts and agreements with the Government Plaintiffs contain misleading or false information about the government exclusivity of the services provided.

225. Microsoft Corporation's August 1, 2016 Enterprise Enrollment agreement with the City of Vallejo, California, defines the term "Community" as:

> the community consisting of one or more of the following: (1) a Government, (2) an Enrolled Affiliate using eligible Government Community Cloud Services to provide solutions to a Government or a qualified member of the Community, or (3) a Customer with Customer Data that is subject to Government regulations for which Customer determines and Microsoft agrees that the use of Government Community Cloud Services is appropriate to meet Customer's regulatory requirements.

Ex. 58, Vallejo Microsoft Agreement, at 5. The amendment also defines "Government Community Cloud" as "Microsoft Online Services that are provisioned in Microsoft's multi-tenant data centers for exclusive use by or for the Community and offered in accordance with the National Institute of Standards and Technology (NIST) Special Publication 800-145." Ex. 58, Vallejo Microsoft Agreement, at 6.

226. The same or virtually identical definitions are put forth in the following contracts and agreements between Defendants and the Government Plaintiffs:

[27] *Available at* http://about.usps.com/handbooks/as805/as805c3_013.htm

Government Plaintiff	Contracting Agency or Division of Government Plaintiff	Date of Contract or Agreement	Agreement Name or Contract Number	Defendant Signatory to Contract or Agreement	Exhibit Number and Page(s)
State of California	Los Angeles County Community Development Commission	8/28/2015	U.S. Government Community Cloud Enterprise Enrollment	Microsoft Corp.	Ex. 49, p. 42
State of California	Los Angeles County Community Development Commission	6/21/2016	Server & Cloud Enrollment	Microsoft Corp.	Ex. 59, p. 4
State of California	Riverside County	11/1/2016	State and Local Enterprise Enrollment	Microsoft Corp.	Ex. 34, pp. 45–46
State of California	Stanislaus County	5/11/2017	State and Local Enterprise Enrollment	Microsoft Corp.	Ex. 37, pp. 36–37
State of Delaware	City of Wilmington	9/17/2018	Volume Licensing Agreement	Microsoft Corp.	Ex. 60, pp. 5–6
State of Florida	Nassau County	11/21/2017	State and Local Enterprise Enrollment	Microsoft Corp.	Ex. 61, pp. 5–6
State of Florida	Pinellas County	6/30/2015	U.S. Government Community Cloud Enterprise Enrollment	Microsoft Corp.	Ex. 40, p. 24
State of Florida	City of Jupiter	November 2016	State and Local Enterprise Enrollment	Microsoft Corp.	Ex. 62, pp. 5–6
State of Florida	City of Miramar	2018	State and Local Enterprise Enrollment	Microsoft Corp.	Ex. 41, pp. 10–11
State of Illinois	City of Bloomington	2018	State and Local Enterprise Enrollment	Microsoft Corp.	Ex. 43, pp. 5–6
State of Nevada	City of Las Vegas Metropolitan Police Department	8/1/2016	State and Local Enterprise Enrollment	Microsoft Corp.	Ex. 63, pp. 7–8

Government Plaintiff	Contracting Agency or Division of Government Plaintiff	Date of Contract or Agreement	Agreement Name or Contract Number	Defendant Signatory to Contract or Agreement	Exhibit Number and Page(s)
State of Montana	Ravalli County	10/29/2015	State and Local Enterprise Enrollment	Microsoft Corp.	Ex. 64, pp. 10–11
State of Nevada	City of Sparks	2015	State and Local Enterprise Enrollment	Microsoft Corp.	Ex. 57, pp. 1–2
State of Nevada	City of Sparks	2015	U.S. Government Community Cloud Enterprise Enrollment	Microsoft Corp.	Ex. 57, p. 13
State of New Mexico	Los Alamos County	2015	U.S. Government Community Cloud Enterprise Enrollment	Microsoft Licensing, G.P.	Ex. 45, p. 6
State of Tennessee	City of Memphis	6/19/2015	Enterprise Subscription Enrollment for U.S. Government Community Cloud, Amendment M306	Microsoft Corp.	Ex. 65, p. 2

227. NIST Special Publication 800-145 defines "community cloud" as a cloud which "is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations)." Ex. 3, NIST Special Publication 800-145, at 7. In contrast, NIST Special Publication 800-145 defines "public cloud" as a cloud which "is provisioned for open use by the general public" and "hybrid cloud" as "a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities but are bound together

by standardized or proprietary technology that enables data and application portability[.]"[28] Ex. 3, NIST Special Publication 800-145, at 7.

228. The GCC cloud services provided by Defendants to the Government Plaintiffs clearly do not comply with the definition of "community cloud" provided by NIST Special Publication 800-145, because AAD—used by all GCC services—operated and stored data in the general commercial cloud. Other components as well—including RMS, Intune, and CAS—operated in the general commercial cloud.

229. As a result, it is inaccurate to characterize the cloud offering contracted for as a "community cloud" under NIST Special Publication 800-145. Microsoft Corporation therefore made false statements in its agreements with the Government Plaintiffs.

230. Furthermore, statements that the services are provisioned for the "exclusive" use of the community are false, as components of those services operated in the commercial cloud. The Azure commercial cloud is not "exclusive" to a government community.

231. Defendants made similar or identical false statements in other contracts and agreements, currently unknown to Relator, under which the sales described in Section V(B) *supra* took place.

C. Defendants made false certifications in their contracts and agreements with the Government Plaintiffs.

232. Defendants' contracts and agreements with the Government Plaintiffs also make false certifications.

233. Defendants' certifications of compliance with laws, ordinances, and the rules and regulations of any government entity are false. *See* Section VII(D)(1) *supra*. These

[28] Some Microsoft marketing materials refer to "hybrid" services as those which combine on-site physical servers with cloud functionality. This is a different definition of "hybrid cloud" than that utilized by NIST.

certifications are false because Defendants' fraudulent conduct violated laws, ordinances, and/or government rules and regulations, including but not limited to federal, state, and local procurement laws.

234. Defendants' certifications that products furnished would conform with the descriptions furnished by Defendants (described *supra* in Section VII(D)(2)) are false because of the aforementioned false statements in Microsoft's marketing and advertising materials concerning GCC.

235. Defendants made similar false certifications in other contracts, currently unknown to Relator, under which the sales described in Section V(B) *supra* took place.

IX. RETALIATION AGAINST RELATOR

236. Defendant Microsoft Corporation retaliated against Relator in response to his reports of, and efforts to stop, the ongoing fraud against the Government Plaintiffs. Relator's first performance evaluation in September 2016, predating his supervisors' knowledge of his reports of fraud, was positive. Relator began to report fraud against the Government Plaintiffs—security issues with GCC and deceptive marketing regarding the exclusivity of the government cloud—continuously, beginning in September of 2016. Once Relator's supervisors learned of his reports of and efforts to stop fraud against the Government Plaintiffs, Relator's performance evaluations became strikingly negative, even though his job performance had not changed since the time he received his initial positive evaluation. Furthermore, Relator's supervisors harassed Relator and made it difficult for him to perform his job duties. Relator's negative evaluation feedback made it impossible for him to obtain a transfer within Microsoft. Thus, when his position was eliminated, Relator was effectively terminated from his employment at Microsoft.

A. Relator starts working for Microsoft and earns positive evaluations

237. Before working for Microsoft Corporation, Relator worked for an Israeli company, Secure Islands. Secure Islands was acquired by Microsoft Corporation in January of 2016, and all of its employees became employees of Microsoft. Secure Islands developed a product which Microsoft renamed Azure Information Protection ("AIP") and utilized in its cloud computing service offering.

238. Relator began working for Microsoft Corporation on January 4, 2016. Relator was initially assigned to work with accounts mostly in the New York area and make them aware of the upcoming offerings. At the beginning of Microsoft's next fiscal year in July 2016, Relator was assigned to be the Financial Global Black Belt ("GBB") expert for AIP and CAS. During the first few weeks of this period, Relator worked out of Microsoft's office in New York City most days of the week. Subsequently, Relator was transferred to a different GBB group and worked from his home in New Jersey. Relator's new group was the Public Sector team, which covered sales to federal, state, and local governments. Relator was responsible for sales to the East Coast for a few months, and then was assigned to cover the whole United States.

239. In his new role as a Security GBB, Relator was responsible for being knowledgeable about AIP and CAS, and identifying and removing any sales "blockers" for those products. A "blocker" is Microsoft's internal terminology for anything that prevents a sale or contract signing with regard to a product or service, either tactically for individual accounts or for an entire market segment, such as Finance, Federal, or State & Local Government ("SLG").

240. Relator worked with other sales teams and departments at Microsoft during his employment, because these other teams all negotiated contracts for or worked with EMS, including the SLG team, Education team, and Federal ("FED") team.

241. Michael Nicosia, Vice President of Global CAS Sales, was Relator's direct supervisor from mid-July of 2016 until October of 2016.[29]

242. Relator's supervisors from October of 2016 until the end of his employment were Senior Director of Solution Sales Kevin Bognar ("Bognar") and Amrit Pal "Roger" Singh ("Singh"), Director of Solution Sales

243. Relator first learned that GCC operated and stored data partially within the Azure commercial cloud at a Microsoft internal conference for its Public Sector division in August of 2016. At this time, Relator had been told that government customers were aware of the fact that their identities resided in the Azure commercial cloud.

244. In September of 2016, Relator underwent a "Connect"—Microsoft's term for mandatory periodic employee evaluations. Relator's supervisor at the time, Michael Nicosia ("Nicosia"), wrote that Relator could use more training in certain aspects, and agreed with Relator's own suggested areas of improvement. *See* Ex. 15, September 2016 Connect, at 7–8, 11, 14–15. However, the majority of Nicosia's comments were positive, like the following:

> John is extremely detailed; incredibly observant and is very thorough in his approach to his role. . . . He has integrated himself very well into the new org[anization]. . . . I feel John did a nice job introducing himself, his new role and responsibilities to provide value add. He is definitely beginning to build the necessary relationships to be successful in the future quarters. He has integrated himself into the [Global Black Belt] community and building good relationships and getting to understand the [Microsoft] ecosystem. Although John has not had too much time to present . . . or had many transformative wins; he has been involved in a number of deals . . . which have resulted into revenue. . . . I feel John has done a good job setting the foundation for success in the coming quarters; it is now time to execute.

Ex. 15, September 2016 Connect, at 7–8. Nicosia also emphasized the need for training and education, stating that Relator "would benefit from additional training" regarding EMS, and

[29] Prior to that, Relator was supervised by Aki Eldar and Kristie Atwood in succession.

should work with his pending new manager, Singh, to "seek out as much training as possible." Ex. 15, September 2016 Connect, at 11, 14.

B. Relator's fraud reports and efforts to stop fraud begin

245. On September 2, 2016, Relator e-mailed Adrian Michels (at that time, Microsoft's Worldwide Enterprise Device and Mobility Lead), Guri Geva (EMS Senior Solutions Sales Manager), and Nicosia in response to a query about "blockers" for CAS. Ex. 16, E-mail with Michels and Others (Sept. 2, 2016), at 2. Relator reported that CAS could not be sold because, in part:

> [State and Local Government] and FED use Government Cloud to comply with Gov't standards. This means both [applications] *must communicate with that Cloud instead* and also that CAS *must be in Govt Cloud* to not reveal Govt data from that cloud. CAS can't touch O[ffice]365 Gov't cloud without this." *Id.* (emphasis added).

Id. (emphasis added). In other words, Relator was reporting that CAS could not be sold to government customers because it did not operate completely within a government community cloud, and because it put government data at risk by operating as it did—within the Azure commercial cloud. Relator went on to describe the exact information put at risk by CAS: Social Security numbers, credit card numbers, and employee identification numbers. *See id.* Within this same e-mail, Relator reported other issues regarding GCC's operations in the commercial cloud, including that government customers "most concerned about Security/Govt requirements cannot use Commercial Cloud for identity." Ex. 16, E-mail with Michels and Others (Sept. 2, 2016), at 3.

246. During October of 2016, Relator communicated with relevant product and sales teams at Microsoft regarding the need to get AIP and CAS working entirely within GCC, instead of partially operating within the commercial cloud. On October 12, 2016, Relator learned from

Program Manager Rue Limones ("Limones") that government customers "would have to give explicit consent" in order to install CAS because it effectively leaks data into the commercial cloud. Ex. 17, E-mail Chain with Limones (Oct. 13, 2016), at 3.

247. After learning this, Relator suggested to Limones: "rather than getting the customer to explicitly consent to additional risk, what about actually running CAS in the Government cloud so that they don't have to be notified of this [security] gap?" Ex. 17, E-mail Chain with Limones (Oct. 13, 2016), at 1. Relator reported this discussion, and the need to make CAS function entirely in the government cloud, in later e-mail correspondence with Singh and Bognar.

248. In November of 2016, Singh and Bognar traveled to Israel to meet with Adallom and Secure Islands management regarding CAS and AIP. Although Relator had discussed with Singh that the security issues with CAS and AIP for the government cloud were a priority, Relator learned on November 15, 2016 that neither Singh nor Bognar had discussed these issues at their meetings in Israel. *See* Ex. 18, E-mail with Singh (Jan. 17, 2017), at 3.

C. The PANYNJ incident

249. In January of 2017, Microsoft's State and Local Government sales team ("SLG") met with the Port Authority of New York and New Jersey ("PANYNJ")—a New York and New Jersey state agency—regarding adding EMS to their existing Microsoft GCC subscription. The team's plan was to utilize PANYNJ as a "test" customer for AIP and other EMS features.

250. AIP operates partially in the Azure commercial cloud. At that time, for PANYNJ or any GCC customer to use AIP, its administrator would have to log in through the Azure commercial cloud portal. Around January 17, 2017, Relator, Azure RMS Senior Program Manager Michael Levin ("Levin"), and Microsoft's NYC Cloud Strategist Mohammed

Abdelhadi ("Abdelhadi") spoke to PANYNJ via telephone about installing AIP. Relator and Levin directed PANYNJ's administrator to log in to the commercial Azure portal in order to install AIP. On this call, Microsoft's contacts at PANYNJ became concerned. They reacted with surprise that their alleged "government-only" username and password allowed them to log in to the commercial cloud, and that their alleged "government-only" user information appeared in the commercial cloud. Microsoft's PANYNJ contacts then asked where their identities were kept, and how they could tell. They also questioned what other services were not in the government cloud.

251. Around this time, Microsoft directed Relator and others to put marketing and sales of AIP and CAS to GCC customers "on hold"—not because of security issues, but because installing these products would cause GCC customers to realize that their identities resided in the commercial cloud. However, sales of GCC and EMS continued—despite the fact that those services also utilize the commercial cloud. Furthermore, EMS automatically includes CAS—it just requires activation by the customer.

252. On January 17, 2017, Relator e-mailed Singh regarding sales issues with AIP and CAS. *See* Ex. 18, E-mail with Singh (Jan. 17, 2017). Although sales of freestanding AIP and CAS to Federal, state, and local government customers had been halted, Relator explained that this very sector was the largest customer for EMS. Ex. 18, E-mail with Singh (Jan. 17, 2017), at 1. Relator's main job duty was to identify and remove "blockers"—issues blocking sales of AIP and CAS. Thus, unless the security issues and blockers could be addressed, Relator could not effectively sell AIP and CAS and achieve the successes demanded by his position.

253. Relator, in order to fulfill his objective to remove "blockers," continued to push Microsoft to solve security issues and integrate a true government cloud version of AIP and

CAS, so that sales could happen without misleading customers or compromising security. During weekly telephone calls with Singh, however, Relator was discouraged from seeking a solution.

254. When Relator was told of new sales opportunities, he would respond to the sales team that the opportunity should only be pursued if the GCC customer at issue knew that their identity was in the commercial cloud, because the team should realize that in the course of demonstrating AIP, the customer would notice that their identities were in the commercial cloud. It troubled Relator that this then seemed to cause those sales teams to end the pursuit of those opportunities, indicating that the customers did not know the truth about their GCC environment, and that Microsoft did not wish for them to find out.

255. Relator followed up on the PANYNJ issue with Singh, Levin, and other Microsoft employees in a January 18, 2017 e-mail:

> Port Authority was asking where their identities were being kept as well as how they could tell, and what else was not in the government cloud that they were seeing [in] their Gcc.us portal.
> Michael Levin confirmed (internally) that there is NO copy of their identities in Fairfax [the true government cloud], their identities are purely in commercial cloud.
>
> And when I look at items such as [a public Microsoft website describing GCC offerings] which show 'YES' for "Cloud Identity" in all flavors of US Government Community offerings without notice of 'not in government cloud', I could now understand the customer's confusion. They see it all in their .us government portal as if it[']s in the government cloud, as well as in the [Microsoft GCC website], and only because they also see the data when they authenticate into the commercial .com portal to access CAS or AIP for instance, can they see that obviously it is in the public cloud (or a copy). . . . Need to discuss how to respond to Port Authority, and what this may mean to other customers.

Ex. 19, E-mail Chain with Singh and Others (Jan. 22, 2017), at 2.

256. Relator scheduled a Skype meeting for the following day with Singh and others to discuss this issue further. *See id.* Those who were included in this e-mail chain, and attended

the meeting, were Singh, Levin, Abdelhadi, National Director of SLG EMS Sales Scott Villinski ("Villinski"), Director of Productivity Sales Julie Kapp ("Kapp"), National Director of Windows Devices & EMS/Security Phil West ("West"), Public Sector Senior Licensing Manager Lisa McNamara, and EMS Technical Sales Professional Lori Chaconas. *See* Ex. 19, E-mail Chain with Singh and Others (Jan. 22, 2017), at 1–2.

257. At this time, based on what superiors like Julie Kapp told him, Relator believed that government customers knew or should have known that their identities or other operations were in the Azure commercial cloud. In particular, Kapp told Relator that SLG customers' contracts specified which services were in the government cloud. Relator would only later discover that this was untrue.

258. On January 24, 2017, Relator received an e-mail raising concerns about another possible "'Port Authority Moment'", referencing what had occurred with PANYNJ. Ex. 66, E-mail Chain with Kelbley and Others (Jan. 24, 2017), at 3). Relator responded, inquiring whether customers truly knew if their identities were in the commercial cloud, and suggesting that this issue be "covered up front[.]" Ex. 66, E-mail Chain with Kelbley and Others, at 2. John Kelbley ("Kelbley"), Cloud Solution Specialist for the SLG team, responded:

> Please let me be clear, WE NEED TO STOP MAKING A BIG DEAL ABOUT THE AIP PORTAL BEING IN COMMERCIAL . . .
> Sashimi is raw fish, but that's not how it is 'presented' to customers. How identities are stored and accessed is a fact not a question, and that is the available deployment mode for AIP. . . . We do not need to create unnecessary conflict controversy in the minds of our customers.

Ex. 66, at 1–2.

D. Retaliation begins

259. On January 25, 2017, Relator met with Bognar and Singh in Scottsdale, Arizona to briefly discuss Relator's career and issues revolving around the sale of AIP and CAS to government customers. Relator had organized the meeting in order to inform Bognar of positive developments regarding Relator's efforts to make AIP and CAS saleable to government customers while remaining in compliance with security standards. As Relator was telling Bognar about his achievements in this regard, Bognar interrupted and attacked Relator for his lack of sales. Bognar told Relator that the security issues with selling AIP and CAS to government customers "are 'bigger than us[.]'" Ex. 20, E-mail Chain with Singh and Others (Feb. 3, 2017), at 4. However, Singh also told Relator to continue to address blockers with the appropriate team members. *See id.* Relator was directed to create a revised business plan and submit it to Singh and Bognar.

260. While travelling with Relator after the discussion in Scottsdale, Bognar advised Relator that he should look for another job outside of Microsoft. Following this discussion, Relator contacted Microsoft's Human Resources department to discuss alternative positions within Microsoft. Amee Matles, a human resources employee, advised Relator that he could look at internal opportunities within Microsoft, but should not "put all of his eggs in one basket", and should also look at working for competitors.

261. On January 31, 2017, Relator e-mailed Phil West, U.S. EMS Business Lead Nishkala Duddu ("Duddu"), Singh, and others, noting the need for Microsoft to obtain customer consent or utilize a warning "splashscreen" to notify customers when they were leaving the government cloud or utilizing services in the commercial cloud. Ex. 21, E-mail Chain with West and Others (Jan. 31, 2017), at 1.

262. On February 1, 2017, Relator teleconferenced with Singh. Relator presented his revised business plan for the fiscal year, outlining his efforts to make AIP and CAS saleable to government clients as well as other recent successes and future plans. Singh did not acknowledge Relator's positive achievements, instead stating that he would wait for feedback from others in Relator's upcoming Connect evaluation. *See* Ex. 22, E-mail Chain with Singh (Feb. 3, 2017), at 2. Following the presentation, Singh directed Relator to include Singh in all future telephone calls, both internal and external. Additionally, although Relator had previously been instructed to seek as much training as possible, Bognar and Singh refused to let Relator attend an upcoming semi-annual training event. *See id.*

263. On February 2, 2017, Relator e-mailed Microsoft's compliance department regarding the issues that he had discussed with Bognar and Singh.

264. On February 3, 2017, Relator replied to an e-mail from Singh and Bognar regarding the January 25, 2017 meeting in Scottsdale. *See* Ex. 20, E-mail Chain with Singh and Bognar (Feb. 3, 2017), at 1–4. Relator reiterated issues with selling EMS to government customers, specifically that customers would discover that components of GCC operated in the commercial cloud. *See* Ex. 20, E-mail Chain with Singh and Bognar, at 2–3. Relator stated, "being attacked each time I even mention these things doesn't seem fair[.]" Ex. 20, E-mail Chain with Singh and Bognar, at 2. Relator also summarized his efforts to devise a solution to sell AIP and CAS while remaining in compliance "from a security standpoint." Ex. 20, E-mail Chain with Singh and Bognar, at 3.

265. On February 10, 2017, after returning from a one-week leave of absence, Relator discovered that Microsoft's compliance department had posted the comments that Relator sent in a public work mailbox visible by everyone at Microsoft—including Singh and Bognar. At this

time, another employee relayed an instruction from Singh to Relator not to sell AIP to government customers because it was not worth the risk of the customer discovering that identities were stored in the commercial cloud.

266. On February 16, 2017, Relator e-mailed Kelbley regarding the issue with PANYNJ:

> The issue is we must tell them they are logging into the non-gcc commercial Cloud to administer [a]ip from a safety and honesty perspective. They then are told they can use their gcc id/password to do So. . . . Then they login to that commercial Cloud and see the rest of their identities. Another flag for them. We were operating this whole time on the understanding that customers knew their identities were in the commercial Cloud, and the big question is whether other customers would freak out similarly. What do you think?

Ex. 23, E-mail Chain with Kelbley (Feb. 16, 2017), at 2–3.

267. On February 17, 2017, Singh e-mailed Relator, ordering him to include Singh on as many internal and external phone calls as possible, and to report to Singh weekly regarding his "key activities." Ex. 24, E-mail with Singh (Feb. 17, 2017), at 1. On February 21, 2017, Relator e-mailed Microsoft's compliance department to report Singh's actions as retaliation.

268. On February 21, 2017, Relator sent an extensive summary of potential safety and security issues with AIP and CAS to a group including Villinski, Duddu, Levin, West, and Limones. *See* Ex. 25, E-mail Chain with Villinski and Others (Feb. 21, 2017), at 1–2. In summary, Relator stressed the importance of informing GCC customers that some data might leak into the commercial cloud, utilizing splashscreens or other warnings to alert GCC users when they leave the government cloud, and to make sure that GCC customers understood which components operated in the commercial cloud. *See id.*

E. Relator's first negative Connect performance review

269. Relator's next Connect evaluation took place on February 22, 2017. Relator had solicited comments from other employees, per Microsoft procedure, for his Connect. Relator asked for comments from employees with whom he had a positive relationship. Singh, however, not only limited Relator's comment requests to certain employees, but also deliberately picked only negative comments to report at Relator's Connect. *See* Ex. 26, February 2017 Connect, at 8–9. Singh's own comments were also largely negative. *See* Ex. 26, February 2017 Connect. It was during this Connect that Relator learned, for the first time, that he and Levin were being "blamed" for "unselling" EMS to PANYNJ.

270. Singh also flagged Relator's Connect with an "Insufficient Results" marker. *See* Ex. 26, February 2017 Connect, at 13. Having "Insufficient Results" means that extra approval is required from a Microsoft Vice President in the employee's old and new departments in order for any job transfer to occur.

271. On March 31, 2017, Relator e-mailed Director of Product Marketing Adam Baron ("Baron") about a presentation Baron had recently given about EMS product offerings. *See* Ex. 27, E-mail Chain with Baron (Mar. 31, 2017), at 1–2. Relator CC'd Singh, West, and Product Marketing Manager Brian Levenson. Ex. 27, E-mail Chain with Baron (Mar. 31, 2017), at 1. Relator outlined how certain slides in Baron's PowerPoint could mislead government customers as to how AIP, CAS, and other EMS components operate. *See id.* Relator noted that customers should be informed about the commercial cloud issues "to minimize surprise and issues[.]" Ex. 27, E-mail Chain with Baron (Mar. 31, 2017), at 1. Relator also discussed the security issue with CAS leaking data into the commercial cloud and the need to notify customers when they leave a secure area of the government cloud. *See* Ex. 27, E-mail Chain with Baron (Mar. 31, 2017), at 2.

272. On April 3, 2017, Relator e-mailed Singh and others, reporting potential security and compliance issues with CAS:

> All content is being sent to CAS for DLP processing from the Government cloud to outside [in the commercial cloud]. What country is this being done in, and/or what standards is CAS meeting (Fedramp level, IRS 1075, CJIS, etc?). Will customers realize their data is leaving and they are using a non-Az[ure]Gov[ernment]-datacenter application when they activate it from Microsoft Azure Government console, opening AzGov up to concerns? . . .
> We are basically suggesting that we protect their info in the government cloud (GCC) by having it all sent outside the government cloud for analysis in the crossover mode. . . .
> I was also concerned because even if you block particular info from [CAS] logs, [CAS does] log that forbidden info . . . really making the security exposure of revealing that info outside the AzGov network even worse. (And another reason why I think we want to make sure customer[s] realize they're running CAS outside [Azure Government] when they turn it on in the AzGov console).

Ex. 28, E-mail Chain with Meyer and Others (Apr. 3, 2017), at 1–4.

273. On April 6, 2017, Relator, Singh, and Baron teleconferenced via Skype and discussed GCC. Relator was told by Singh and Baron that AIP revealed issues with GCC that Microsoft did not want exposed to the customer, and that as a result, they would postpone sales of AIP. At that time, Relator realized for certain that what the SLG and FED team had told him was false—Microsoft had not told government customers that their identities resided in the commercial cloud.

274. In early April of 2017, Relator sent several e-mails to Microsoft's compliance department reporting that he had been retaliated against for revealing issues with GCC.

275. On May 24, 2017, Relator e-mailed Singh a list of Relator's accomplishments during the 2017 fiscal year. *See* Ex. 29, E-mail with Singh (May 24, 2017), at 1. Relator noted the following after listing his accomplishments, reiterating security issues with GCC and deception regarding the government cloud:

> Although Sales teams assured us that GCC customers were aware that their identities were in the regular commercial cloud, we found out this was not the case, which then minimized the impact the AIP solution could have for [Fiscal Year] 2017. As part of trying to address this, however, [the] other impact was that I was able to document a number of issues[.] . . . These include that actual users&Admins don't see contracts where exclusions or info conflicting with info in [the government] consoles are stated; Marketing materials commingling true government cloud benefits with GCC which does not have them; GCC Users & Admins not being aware that Intune and CAS [are] operating in regular Commercial Cloud for them because they show up in a Government Cloud console; . . . Identities showing up as if they are in GCC, etc. My Impact being that [Microsoft] has a chance to get ahead of these issues before sensitive customer data is leaked because of this; . . . or States/Fed make issues for refunds or damages, etc.

Ex. 29, E-mail with Singh (May 24, 2017), at 1–2.

F. Retaliation continues with a second "Insufficient Results" notation

276. Relator's final Connect for fiscal year 2017 took place on June 2, 2017. Although Singh included one or two positive comments from Relator's coworkers in his comments, Singh's own comments are negative. *See* Ex. 30, June 2017 Connect. Singh flagged Relator's Connect with an "Insufficient Results" marker again, stressing that Relator needed to make more sales. *See* Ex. 30, June 2017 Connect, at 19.

277. On June 6, 2017, Relator e-mailed Levin and RMS Senior Program Manager Aashish Ramdas ("Ramdas") about security issues with GCC, deception of government customers regarding GCC's components that operated in the commercial cloud, and his efforts to find a solution. *See* Ex. 31, E-mail Chain with Singh and Others (June 7, 2017), at 1–3.

278. On June 23, 2017, Relator e-mailed Singh and the GBB responsible for tracking open GCC product issues, David Case ("Case"), about security and compliance issues revolving around AIP, CAS, and GCC. *See* Ex. 1, E-mail with Singh & Case (June 23, 2017), at 1–2. Relator discussed CAS' data leakage issue and how Microsoft was misleading government customers about GCC operations occurring in the commercial cloud. Ex. 1, E-mail with Singh &

Case (June 23, 2017), at 1–2. Relator emphasized that Microsoft was deceiving GCC customers as to where their user identities were stored:

> Identities for GCC customers – this has been a big project. Moving them was considered. I'm not dictating where or how this is resolved, the issue is that
> i. we SHOW CUSTOMERS THEIR IDENTITIES ARE IN THE GOV CLOUD IN THE GOV CONSOLE, WHICH IS NOT TRUE
> ii. datasheets and marketing materials and [Microsoft's website] reflect same, which is not true, comingling gcc and defense information together.

Ex. 1, E-mail with Singh & Case (June 23, 2017), at 1.

G. Relator is effectively terminated

279. On July 6, 2017, Relator received a letter informing him that his position was "being eliminated." Ex. 32, Termination Letter (July 6, 2017), at 1. The letter stated that Relator's termination would become effective on September 4, 2017. *Id.* The letter included a severance agreement, which Relator never executed.

280. That same day, Relator also received a phone call from Bognar and HR Manager Katie Seager informing him that his position was being eliminated, but with no explanation as to why.

281. Other employees whose positions were eliminated at the same time were all transferred to other positions within Microsoft in July of 2017, including Heather Caban, Eran Abramovitz, David Gifford, Kim Beetlestone, Amir Gabrieli, and Stuart Dankevy. Relator, however, was not offered a new position. Relator had requested a transfer, but was told that this would not be possible because of Singh's "Insufficient Results" notation on Relator's February and June Connects.

H. Relator continues to contact superiors at Microsoft despite his pending termination, hoping to stop fraud against the Government Plaintiffs

282. Between July 6, 2017 and September 4, 2017, Relator continued to be paid but did not perform any work for Microsoft Corporation. Relator was instructed not to perform and work and was removed from Microsoft's corporate networks. However, Relator did send correspondence to vice presidents and other superiors at Microsoft regarding the security issues he observed with GCC, hoping to put an end to GCC's security defects and the deception of government customers. *See, e.g.*, Ex. 33, E-mail Chain with Bharat Shah (July 6, 2017), at 1; Ex. 36, E-mail Chain with Bharat Shah and Dan Plastina (July 6, 2017), at 1–2.

283. For example, on the night of July 6, 2017, Relator forwarded e-mail correspondence explaining the security issues with GCC to Bharat Shah, Microsoft's Vice President of Security. *See* Ex. 33, E-mail Chain with Bharat Shah (July 6, 2017), at 1. Relator also e-mailed Dan Plastina, Microsoft's Partner Director of Threat Protection, regarding GCC's security issues. *See* Ex. 36, E-mail Chain with Bharat Shah and Dan Plastina (July 6, 2017), at 1–2.

284. As a direct consequence of his reports of fraud on government customers and efforts to prevent both fraudulent inducement of contracts and fraud under existing contracts, Relator was retaliated against with harassment and termination from his position at Microsoft Corporation.

X. ACTIONABLE CONDUCT BY DEFENDANTS

A. False Claims Act

1. Applicable Law

285. This is an action to recover damages and civil penalties on behalf of the United States and Relator arising from the false and/or fraudulent statements, claims, and acts that Defendants made in violation of the False Claims Act ("FCA"), 31 U.S.C. §§ 3729–3732.

286. The FCA provides that any person who:

> (A) knowingly presents, or causes to be presented, a false and/or fraudulent claim for payment or approval; [or]
> (B) knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim; [or]
> (C) conspires to commit a violation of [the FCA,]

31 U.S.C. § 3729(a)(1), is liable to the United States for a civil penalty of not less than $11,181 and not more than $22,363 for each such claim, plus three times the amount of damages sustained by the United States, including consequential damages, sustained by the Government because of the FCA violation. *See id.*; 28 C.F.R. § 85.5.

287. The FCA defines "claim" as:

> any request or demand, whether under a contract or otherwise, for money or property and whether or not the United States has title to the money or property, that—
>
> (i) is presented to an officer, employee, or agent of the United States; or
>
> (ii) is made to a contractor, grantee, or other recipient, if the money or property is to be spent or used on the Government's behalf or to advance a Government program or interest, and if the United States Government—
>
> (A) provides or has provided any portion of the money or property requested or demanded; or

> (IB) will reimburse such contractor, grantee, or other recipient for any portion of the money or property which is requested or demanded[.]

31 U.S.C. § 3729(b)(2).

288. The FCA allows any person having knowledge of a false and/or fraudulent claim against the United States to bring an action in a U.S. federal district court for himself and for the United States, and to share in any recovery, as authorized by 31 U.S.C. § 3730.

289. Based on these provisions, Relator Kurzman seeks through this action to recover damages and civil penalties arising from Defendants' violations of the FCA.

2. Defendants' Violations of the False Claims Act

a. Presentation of False and/or Fraudulent Claims (31 U.S.C. § 3729(a)(1)(A))

290. From 2012 to the present, Defendants knowingly presented, or caused the presentment of, false and/or fraudulent claims for payment or approval to the United States.

291. Defendants fraudulently induced the United States, the State of California,[30] and their agencies to enter into federally-funded contracts and agreements for cloud computing services by making false statements regarding the cloud services' government exclusivity and security. Defendants made these false statements in marketing and advertising materials as well as in the contracts and agreements themselves.

292. Defendants also made false certifications in the contracts and agreements at issue as to: (1) compliance with laws; and (2) that Defendants provided the services at issue in conformity with descriptions they provided.

[30] Via the Los Angeles County Community Development Commission, who entered into a contract funded by the U.S. Department of Housing and Urban Development

293. Defendants submitted claims for payment under the contracts and agreements at issue, which were both fraudulently induced and/or contain false statements and certifications.

294. By creating and carrying out their fraudulent scheme, Defendants knowingly and repeatedly violated the False Claims Act. *See* 31 U.S.C. § 3729(a)(1)(A).

295. Defendants' knowing submission, or causation of submission, of false and/or fraudulent claims had the potential to influence the United States' payment decision and was material to the United States' decision to pay the claims.

296. Defendants' misrepresentations regarding the cloud services at issue and their compliance with the applicable standards for cloud computing are material because they went to the very essence of the bargain for which the United States and the State of California contracted. Had the United States known of Defendants' fraudulent non-compliance, which resulted in the submission of ineligible false claims for reimbursement, the United States would not have paid the claims.

297. Defendants' presentment, or causation of presentment, of false and/or fraudulent claims to the United States and the State of California was a foreseeable factor in the United States' loss and a consequence of Defendants' fraudulent scheme. By virtue of Defendants' actions, the United States has suffered damages and is entitled to recover treble damages plus a civil monetary penalty for each false claim.

b. Making or Using False Records or Statements Material to False and/or Fraudulent Claims (31 U.S.C. § 3729(a)(1)(B))

298. From 2012 to the present, Defendants knowingly made, used, or caused to be made or used, false records or statements that were material to false and/or fraudulent claims paid or approved by the United States. These false records or statements include those made on websites and in other marketing materials.

299. Defendants knowingly and fraudulently used the false statements in their marketing materials and websites both to induce the United States and the State of California to enter into the contracts and agreements at issue and to get false and/or fraudulent claims made pursuant to those contracts paid or approved by the United States.

300. By creating and carrying out their fraudulent scheme, Defendants knowingly and repeatedly violated 31 U.S.C. § 3729(a)(1)(B).

301. Defendants' false statements or records, or causation of false statements or records, had the potential to influence the United States' payment decision and were material to the United States' decision to pay the claims.

302. Defendants' false statements regarding the exclusivity and deployment models of the cloud services at issue were material because they went to the very essence of the bargain for which the United States and the State of California contracted. Had the United States and the State of California known of Defendants' fraudulent misrepresentations regarding the cloud services at issue, which resulted in the submission of ineligible false and/or fraudulent claims for reimbursement, then the United States and the State of California would not have entered into the contracts and agreements at issue or paid claims under those contracts and agreements.

303. Defendants' submission, or causation of submission, of false records and statements material to false and/or fraudulent claims was a foreseeable factor in the United States' loss and a consequence of Defendants' scheme. By virtue of Defendants' actions, the United States has suffered actual damages and is entitled to recover treble damages plus a civil monetary penalty for each false claim.

c. Conspiracy (31 U.S.C. § 3729(a)(1)(C))

304. From 2012 to the present, the Reseller Defendants conspired together with Defendants Microsoft Licensing, G.P. and Microsoft Corporation to: (1) fraudulently induce the United States and the State of California to enter into the federally-funded contracts and agreements at issue; and (2) submit or cause the submission of false claims under those contracts and agreements to the United States and the State of California.

305. Microsoft Corporation and Microsoft Licensing, G.P. (collectively "Microsoft") worked in tandem with the Reseller Defendants, entering into agreements with the United States and the State of California which are part and parcel of the actual contracts between the Reseller Defendants and the United States and the State of California.

306. The Reseller Defendants are licensed resellers of Microsoft products. The Reseller Defendants executed all sales contracts for the cloud services at issue in this case, and issued all invoices associated with the contracts at issue.

307. The Reseller Defendants, having issued the invoices for the specific products at issue, knew that cloud services denoted as "GCC" or "for Government" were not part of a government cloud, as the "fake SKU" that Microsoft used for these services includes commercial and government community cloud services.

308. Defendants' conspiracy had the potential to influence the United States' payment decision because the United States and the State of California would not have entered into the contracts and agreements at issue or paid claims under them had they known that they were not receiving true "government cloud" services.

d. Retaliation (31 U.S.C. § 3730(h))

309. Section 3730(h) of Title 31 of the United States Code defines whistleblower protection under the False Claims Act as follows:

> (1) Any employee, contractor, or agent shall be entitled to all relief necessary to make that employee, contractor, or agent whole, if that employee, contractor, or agent is discharged, demoted, suspended, threatened, harassed, or in any other manner discriminated against in the terms and conditions of employment because of lawful acts done by the employee, contractor, agent or associated others in furtherance of an action under this section or other efforts to stop 1 or more violations of this subchapter.an injunction to restrain continued discrimination;
> (2) Relief under paragraph (1) shall include reinstatement with the same seniority status that employee, contractor, or agent would have had but for the discrimination, 2 times the amount of back pay, interest on the back pay, and compensation for any special damages sustained as a result of the discrimination, including litigation costs and reasonable attorneys' fees. An action under this subsection may be brought in the appropriate district court of the United States for the relief provided in this subsection.

310. As discussed *supra*, in violation of 31 U.S.C. § 3730(h)(1), Defendant Microsoft Corporation retaliated against Relator as a result of Relator's lawful acts or other efforts to stop Defendants from committing False Claims Act violations. Defendant Microsoft Corporation punished Relator for his lawful and statutorily protected activity with negative "Connect" reviews, harassment, and, ultimately, termination.

311. Relator's supervisors, Singh and Bognar, urged Relator not to concern himself with AIP and CAS security issues. Despite the fact that Relator's job duties included identifying and removing sales "blockers", especially for CAS and AIP, Singh and Bognar neglected to take action to help fix the security issues with those products. Instead, because CAS and AIP would reveal to GCC customers that their identities (and other GCC components) resided in the commercial cloud, Singh and Bognar took pains to delay or halt sales and marketing of CAS and AIP to GCC customers. Because government customers were the main market for CAS and

AIP, as well as EMS, these actions made it difficult for Relator to perform his job duties and achieve any sales.

312. Singh and Bognar also harassed Relator. Singh requested multiple times that Relator include him on every single telephone call, both internal and external. And, neither Singh nor Bognar recognized any positive achievements on Relator's end when evaluating his job performance. Furthermore, Bognar effectively told Relator that he should leave Microsoft.

313. Despite an initial positive Connect evaluation, after Relator began to report and try to stop Microsoft's fraud, Relator's Connect evaluations became strikingly more negative. Singh selected only negative coworker feedback to use in Relator's February 2017 Connect evaluation, and gave Relator an "Insufficient Results" notation on his February and June 2017 Connects. These actions prevented Relator from transferring to another position within Microsoft, and transformed the elimination of his position into outright termination.

314. In contrast, every other employee whose position was eliminated alongside Relator's obtained a new position within Microsoft.

315. Relator has suffered both economic loss and emotional harm as a result of Defendant Microsoft Corporation's retaliatory actions.

XI. CAUSES OF ACTION

A. Count I – Presentation of False and/or Fraudulent Claims (31 U.S.C. § 3729(a)(1)(A))

316. Relator realleges and hereby incorporates by reference each and every allegation contained in all paragraphs of this Complaint.

317. From 2012 to the present, Defendants have knowingly presented, or caused to be presented, false and/or fraudulent claims for payment or approval to the United States.

318. Defendants fraudulently induced the United States, the State of California,[31] and their agencies to enter into federally-funded contracts and agreements for cloud computing services by making false statements regarding the cloud services' government exclusivity and security. Defendants made these false statements in marketing and advertising materials as well as in the contracts and agreements themselves. Defendants also made false certifications in the contracts and agreements at issue.

319. By creating and carrying out their fraudulent scheme, Defendants knowingly and repeatedly violated the False Claims Act. *See* 31 U.S.C. § 3729(a)(1)(A).

320. Defendants' knowing submission, or causation of submission, of false and/or fraudulent claims had the potential to influence the United States' payment decision and was material to the United States' decision to pay the claims.

321. The United States paid the false and/or fraudulent claims.

322. Defendants' presentment or causation of presentment of false and/or fraudulent claims was a foreseeable factor in the United States' loss and a consequence of Defendants' fraudulent scheme. By virtue of Defendants' actions, the United States has suffered damages and is entitled to recover treble damages plus a civil monetary penalty for each false and/or fraudulent claim.

B. Count II – Making or Using False Records or Statements Material to False and/or Fraudulent Claims (31 U.S.C. § 3729(a)(1)(B))

323. Relator realleges and hereby incorporates by reference each and every allegation contained in all paragraphs of this Complaint.

[31] Via the Los Angeles County Community Development Commission, who entered into a contract funded by the U.S. Department of Housing and Urban Development

324. From 2012 to the present, Defendants knowingly made, used, or caused to be made or used, false records or statements that were material to false and/or fraudulent claims paid or approved by the United States. These false records or statements include those made on websites and in other marketing materials.

325. Defendants knowingly and fraudulently used the false statements in their marketing materials and websites both to induce the United States and the State of California to enter into the federally-funded contracts and agreements at issue, and to get false and/or fraudulent claims made pursuant to those contracts paid or approved by the United States.

326. Defendants' false statements or records, or causation of false statements or records, had the potential to influence the United States' payment decision and were material to the United States' decision to pay the claims.

327. Defendants' false statements regarding the exclusivity and deployment models of the cloud services at issue were material because they went to the very essence of the bargain for which the United States and the State of California contracted. Had the United States and the State of California known of Defendants' fraudulent misrepresentations regarding the cloud services at issue, which resulted in the submission of ineligible false and/or fraudulent claims for reimbursement, then the United States and the State of California would not have entered into the contracts and agreements at issue or paid claims under those contracts and agreements.

328. By creating and carrying out their fraudulent scheme, Defendants knowingly and repeatedly violated 31 U.S.C. § 3729(a)(1)(B).

329. The United States paid the false and/or fraudulent claims.

330. Defendants' submission, or causation of submission, of false records and statements material to false and/or fraudulent claims was a foreseeable factor in the United

States' loss and a consequence of Defendants' scheme. By virtue of Defendants' actions, the United States has suffered actual damages and is entitled to recover treble damages plus a civil monetary penalty for each false and/or fraudulent claim.

C. Count III – Conspiracy (31 U.S.C. § 3729(a)(1)(C))

331. Relator realleges and hereby incorporates by reference each and every allegation contained in all paragraphs of this Complaint.

332. From 2012 to the present, Defendants Microsoft Corporation and Microsoft Licensing, G.P. conspired together with the Reseller Defendants, in violation of the False Claims Act: (1) to fraudulently induce the United States and the State of California to enter into federally-funded contracts and agreements; and (2) to submit false claims under those contracts to the United States for payment.

333. Microsoft worked in tandem with the Reseller Defendants, entering into agreements with the United States and the State of California which are part and parcel of the actual contracts between the Reseller Defendants and the United States and the State of California.

334. The Reseller Defendants executed all sales contracts for the cloud services at issue in this case, and issued all invoices associated with the contracts at issue. The Reseller Defendants, having issued the invoices for the specific products at issue, knew that cloud services denoted as "GCC" or "for Government" were not part of a government cloud, as the "fake SKU" that Microsoft used for these services includes commercial and government community cloud services.

335. Defendants' conspiracy had the potential to influence the United States' payment decision because the United States and the State of California would not have entered into the

federally-funded contracts and agreements at issue or paid claims under them had they known that they were not receiving true "government cloud" services.

336. The United States paid the false and/or fraudulent claims.

337. Defendants' conspiratorial scheme was a foreseeable factor in the United States' loss. Due to Defendants' actions, the United States has suffered actual damages and is entitled to recover treble damages plus a civil monetary penalty for each false and/or fraudulent claim.

PRAYER FOR RELIEF

338. WHEREFORE, Relator prays that this Court enter judgment against Defendants and award the following:

(1) Damages in the amount of three (3) times the actual damages suffered by the United States as a result of Defendants' conduct;

(2) Civil penalties against Defendants up to the maximum allowed by law for each violation of 31 U.S.C. § 3729;

(3) The maximum award Relator may recover pursuant to 31 U.S.C. § 3730(d);

(4) All costs and expenses of this litigation, including attorneys' fees and costs of court; and

(5) All other relief that the Court deems just and proper.

D. Count IV – Retaliation (31 U.S.C. § 3730(h))

339. Relator realleges and hereby incorporates by reference each and every allegation contained in all paragraphs of this Complaint.

340. In violation of 31 U.S.C. § 3730(h), Defendant Microsoft Corporation retaliated against Relator Kurzman as a result of lawful acts he committed in furtherance of efforts to stop Defendants from committing violations of the False Claims Act.

341. Microsoft Corporation punished Relator for his lawful and statutorily protected activity with harassment and termination.

342. Relator has suffered economic loss and emotional harm as a result of his termination by Microsoft Corporation.

PRAYER FOR RELIEF

343. WHEREFORE, Relator prays that this Court enter judgment against Defendant Microsoft Corporation for the following:

(1) Reinstatement with the same seniority status;

(2) Two times the amount of Relator's back pay;

(3) Interest on Relator's back pay;

(4) Compensation for special damages sustained by Relator as a result of Defendants' actions, including but not limited to compensatory damages for emotional pain, suffering, inconvenience, mental anguish, loss of enjoyment of life, loss to reputation, and other pecuniary and nonpecuniary losses;

(5) Punitive damages;

(6) Litigation costs and attorneys' fees;

(7) Prejudgment interest; and

(8) Any other relief that the Court deems just and proper to make the Relator whole.

E. Count V – District of Columbia Procurement Reform Amendment Act

344. Relator realleges and hereby incorporates by reference each and every allegation contained in all paragraphs of this complaint.

345. This is a *qui tam* action brought by Relator and the District of Columbia to recover treble damages and civil penalties under the District of Columbia Procurement Reform Amendment Act ("DCFCA"), D.C. CODE §§ 2-381.01–2-381.10.

346. The DCFCA provides that any person who:

(1) knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval; [or]

> (2) knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim; [or] . . .
> (7) conspires to commit a violation of [the DCFCA,]

D.C. CODE § 2-381.02(a), is liable to the District of Columbia ("the District") for a civil penalty of $5,500 to $11,000[32] for each false or fraudulent claim, plus three times the amount of damages which the District of Columbia sustains because of the DCFCA violation. *Id.*

1. Presentment of False and/or Fraudulent Claims (D.C. CODE § 2-381.02(a)(1))

347. From at least 2016 to the present, Defendants Microsoft Corporation and Dell Marketing, L.P. knowingly presented, or caused to be presented, false and/or fraudulent claims to the District.

348. The above-named Defendants fraudulently induced the District to enter into contracts and agreements for cloud computing services by making false statements regarding GCC's government exclusivity and security in marketing and advertising materials and/or in the contracts and agreements themselves. The above-named Defendants then submitted claims for payment under the contracts and agreements at issue, which were both fraudulently induced.

349. The above-named Defendants' knowing submission, or causation of submission, of false and/or fraudulent claims had the potential to influence the District's payment decision and was material to the District's decision to pay the claims.

350. The above-named Defendants' misrepresentations regarding the cloud services at issue are material because they went to the very essence of the bargain for which the District contracted. Had the District known of Defendants' fraudulent non-compliance, which resulted in the submission of ineligible false claims for reimbursement, the District would not have paid the claims.

[32] Or the applicable penalty range after adjusting for inflation pursuant to D.C. CODE § 2-381.10.

351. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the DCFCA.

352. The above-named Defendants' presentment, or causation of presentment, of false and/or fraudulent claims to the District was a foreseeable factor in the District's loss and a consequence of Defendants' fraudulent scheme. By virtue of the above-named Defendants' actions, the District has suffered damages.

2. Making or Using False Records or Statements Material to False and/or Fraudulent Claims (D.C. CODE § 2-381.02(a)(2))

353. From at least 2016 to the present, Defendants Microsoft Corporation and Dell Marketing, L.P. knowingly made, used, or caused to be made or used, false records or statements that were material to false and/or fraudulent claims paid or approved by the District. These false records or statements include those made on websites and in other marketing materials.

354. The above-named Defendants knowingly and fraudulently used the false statements in their marketing materials and websites both to induce the District to enter into the contracts and agreements at issue and to get false and/or fraudulent claims made pursuant to those contracts paid or approved by the District

355. The above-named Defendants' false statements or records, or causation of false statements or records, had the potential to influence the District's payment decision and were material to the District's decision to pay the claims.

356. The above-named Defendants' false statements regarding the exclusivity and deployment models of the cloud services at issue were material because they went to the very essence of the bargain for which the District contracted. Had the District known of Defendants' fraudulent misrepresentations regarding the cloud services at issue, which resulted in the submission of ineligible false and/or fraudulent claims for reimbursement, then the District

would not have entered into the contracts and agreements at issue or paid claims under those contracts and agreements.

357. By creating and carrying out their fraudulent scheme, Defendants Microsoft Corporation and Dell Marketing, L.P. knowingly and repeatedly violated the DCFCA.

358. The above-named Defendants' submission, or causation of submission, of false records and statements material to false and/or fraudulent claims was a foreseeable factor in the District's loss and a consequence of Defendants' scheme. By virtue of Defendants' actions, the District has suffered damages.

3. Conspiracy (D.C. CODE § 2-381.02(a)(7))

359. From at least 2016 to the present, Defendant Dell Marketing, L.P. conspired together with Defendant Microsoft Corporation to: (1) fraudulently induce the District to enter into contracts and agreements with them; and (2) submit or cause the submission of false and/or fraudulent claims under those contracts and agreements to the District.

360. Defendant Microsoft Corporation entered into agreements with the District that are part and parcel of Defendant Dell Marketing, L.P.'s contracts with the District for the cloud services at issue.

361. Defendant Dell Marketing, L.P., having issued all invoices for the specific products at issue, knew that cloud services marketed as "for Government" which utilized Microsoft's "fake SKU" included commercial cloud services, and were therefore not actually "for Government."

362. The above-named Defendants' conspiracy had the potential to influence the District's payment decision because the District would not have entered into the contracts and

agreements at issue or paid claims under them had it known that it was not receiving true "government cloud" services.

* * *

363. WHEREFORE, Relator respectfully requests that the Court enter judgment against Defendants Microsoft Corporation and Dell Marketing, L.P., and award the following:

To the DISTRICT OF COLUMBIA:

a) Three times the amount of damages sustained by the District of Columbia as a result of Defendants' fraudulent and illegal practices;

b) Civil penalties against Defendants up to the maximum allowed by law for each violation of the DCFCA; and

c) All costs incurred in bringing this action.

To RELATOR:

a) The maximum amount allowed pursuant to D.C. CODE § 2-381.03(f) and/or any other applicable provision of law;

b) Reimbursement for reasonable expenses Relator incurred in connection with this action;

c) An award of reasonable attorney's fees and costs; and

d) Such further relief as this Court deems equitable and just.

F. Count VI – California False Claims Act

364. Relator realleges and hereby incorporates by reference each and every allegation contained in all paragraphs of this complaint.

365. This is a *qui tam* action brought by Relator and the State of California to recover treble damages and civil penalties under the California False Claims Act ("California FCA"), CAL. GOV'T CODE §§ 12650–12656.

366. The California FCA provides that any person who:

(1) knowingly presents or causes to be presented a false or fraudulent claim for payment or approval; [or]
(2) knowingly makes, uses, or causes to be made or used a false record or statement material to a false or fraudulent claim; [or]
(3) conspires to commit a violation of [the California FCA]

CAL. GOV'T CODE § 12651(a), is liable to the State of California (or the applicable political subdivision thereof) for a civil penalty of $11,181 to $22,363 for each violation of the California FCA, plus three times the amount of damages which the State of California or political subdivision sustains because of the violation. *See* 28 C.F.R. § 85.5; CAL GOV'T CODE § 12651(a).

1. Presentment of False and/or Fraudulent Claims (CAL. GOV'T CODE § 12651(a)(1))

367. From 2012 to the present, the following Defendants knowingly presented, or caused to be presented, false and/or fraudulent claims to the State of California and its political subdivisions: Microsoft Corporation; CDW Corporation; CompuCom Systems, Inc.; Crayon Software Experts LLC; Dell Marketing, L.P.; En Pointe Technologies Sales, LLC; Insight Public Sector, Inc.; Lilien, LLC; PCM, Inc.; PCMG, Inc.; Planet Technologies, Inc.; ProSum Inc.; Software One, Inc.; Solid Networks Inc.; and Sysorex Government Services, Inc.

368. The above-named Defendants fraudulently induced the State of California and its political subdivisions to enter into contracts and agreements for cloud computing services by making false statements regarding the cloud services' government exclusivity and security. Defendants made these false statements in marketing and advertising materials as well as in the contracts and agreements themselves.

369. The above-named Defendants also made false certifications in the contracts and agreements at issue as to: (1) the truth, completeness, and accuracy of information provided; (2) compliance with laws; and (3) compliance with specified cloud computing standards.

370. The above-named Defendants submitted claims for payment to the State of California and its political subdivisions under the contracts and agreements at issue, which were both fraudulently induced and/or contain false statements and certifications.

371. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the California FCA.

372. The above-named Defendants' knowing submission, or causation of submission, of false and/or fraudulent claims had the potential to influence the State of California and its political subdivisions' payment decision and was material to the State of California and its political subdivisions' decision to pay the claims.

373. The above-named Defendants' misrepresentations regarding the cloud services at issue and their compliance with the applicable standards for cloud computing are material because they went to the very essence of the bargain for which the State of California and its political subdivisions contracted. Had the State of California and its political subdivisions known of Defendants' fraudulent non-compliance, which resulted in the submission of ineligible false claims for reimbursement, they would not have paid the claims.

374. The above-named Defendants' presentment, or causation of presentment, of false and/or fraudulent claims to the State of California and its political subdivisions was a foreseeable factor in the State of California and its political subdivisions' loss and a consequence of Defendants' fraudulent scheme. By virtue of the above-named Defendants' actions, the State of California and its political subdivisions have suffered damages.

2. Making or Using False Records or Statements Material to False and/or Fraudulent Claims (CAL. GOV'T CODE § 12651(a)(2))

375. From 2012 to the present, the above-named Defendants knowingly made, used, or caused to be made or used, false records or statements that were material to false and/or

fraudulent claims paid or approved by the State of California and its political subdivisions. These false records or statements include those made on websites and in other marketing materials.

376. The above-named Defendants knowingly and fraudulently used the false statements in their marketing materials and websites both to induce the State of California and its political subdivisions to enter into the contracts and agreements at issue and to get false and/or fraudulent claims made pursuant to those contracts paid or approved by the State of California and its political subdivisions.

377. The above-named Defendants' false statements or records, or causation of false statements or records, had the potential to influence the State of California and its political subdivisions' payment decision and were material to the State of California and its political subdivisions' decision to pay the claims.

378. The above-named Defendants' false statements regarding the exclusivity and deployment models of the cloud services at issue were material because they went to the very essence of the bargain for which the State of California and its political subdivisions contracted. Had the State of California and its political subdivisions known of Defendants' fraudulent misrepresentations regarding the cloud services at issue, which resulted in the submission of ineligible false and/or fraudulent claims for reimbursement, then the State of California and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under those contracts and agreements.

379. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the California FCA.

380. The above-named Defendants' submission, or causation of submission, of false records and statements material to false and/or fraudulent claims was a foreseeable factor in the State of California's loss and a consequence of Defendants' scheme. By virtue of Defendants' actions, the State of California and its political subdivisions have suffered damages.

3. Conspiracy (CAL. GOV'T CODE § 12651(a)(3))

381. From 2012 to the present, the above-named Defendants conspired together to: (1) fraudulently induce the State of California and its political subdivisions to enter into contracts and agreements with them; and (2) submit or cause the submission of false and/or fraudulent claims under those contracts and agreements to the State of California and its political subdivisions.

382. Microsoft entered into agreements with the State of California and its political subdivisions that are part and parcel of the Reseller Defendants' contracts with the State of California and its political subdivisions for the cloud services at issue.

383. The Reseller Defendants named above, having issued all invoices for the specific products at issue, knew that cloud services marketed as "for Government" which utilized Microsoft's "fake SKU" included commercial cloud services, and were therefore not actually "for Government."

384. The above-named Defendants' conspiracy had the potential to influence the State of California and its political subdivisions' payment decision because State of California and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under them had they known that they were not receiving true "government cloud" services.

* * *

385. WHEREFORE, Relator respectfully requests that the Court enter judgment against Defendants, and award the following:

To the STATE OF CALIFORNIA:

a) Three times the amount of damages sustained by the State of California as a result of Defendants' fraudulent and illegal practices;

b) Civil penalties against Defendants up to the maximum allowed by law for each violation of CAL. GOV'T CODE § 12651; and

c) All costs incurred in bringing this action.

To RELATOR:

a) The maximum amount allowed pursuant to CAL. GOV'T CODE § 12652 and/or any other applicable provision of law;

b) Reimbursement for reasonable expenses Relator incurred in connection with this action;

c) An award of reasonable attorney's fees and costs; and

d) Such further relief as this Court deems equitable and just.

G. Count VII – Delaware False Claims and Reporting Act

386. Relator realleges and hereby incorporates by reference each and every allegation contained in all paragraphs of this complaint.

387. This is a *qui tam* action brought by Relator and the State of Delaware to recover treble damages and civil penalties under the Delaware False Claims and Reporting Act ("DFCA"), 6 DEL. CODE ANN. §§ 1201–1211.

388. The DFCA provides that any person who:

(1) Knowingly presents or causes to be presented a false or fraudulent claim for payment or approval; [or]
(2) Knowingly makes, uses or causes to be made or used a false record or statement material to a false or fraudulent claim; [or]
(3) Conspires to commit a violation of [the above paragraphs,]

6 DEL CODE ANN. § 1201(a), is liable to the State of Delaware for a civil penalty of $11,181 to $22,363 for each violation of the DFCA, plus three times the amount of damages which the State of Delaware sustains because of the violation. *See* 28 C.F.R. § 85.5; 6 DEL. CODE ANN. § 1201(a).

1. Presentment of False and/or Fraudulent Claims (DEL. CODE ANN. § 1201(a)(1))

389. From at least 2013 to the present, Defendants Microsoft Corporation and SHI International Corporation ("SHI") knowingly presented, or caused to be presented, false and/or fraudulent claims to the State of Delaware and its political subdivisions for payment or approval.

390. The above-named Defendants fraudulently induced the State of Delaware and its political subdivisions to enter into contracts and agreements for cloud computing services by making false statements regarding the cloud services' government exclusivity and security. Defendants made these false statements in marketing and advertising materials as well as in the contracts and agreements themselves.

391. The above-named Defendants also made false certifications in the contracts and agreements at issue as to: (1) the truth, completeness, and accuracy of information provided; and (2) compliance with laws.

392. The above-named Defendants submitted claims for payment to the State of Delaware and its political subdivisions under the contracts and agreements at issue, which were both fraudulently induced and/or contain false statements and certifications.

393. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the DFCA.

394. The above-named Defendants' knowing submission, or causation of submission, of false and/or fraudulent claims had the potential to influence the State of Delaware and its

political subdivisions' payment decision and was material to the State of Delaware and its political subdivisions' decision to pay the claims.

395. The above-named Defendants' misrepresentations regarding the cloud services at issue and their compliance with the applicable standards for cloud computing are material because they went to the very essence of the bargain for which the State of Delaware and its political subdivisions contracted. Had the State of Delaware and its political subdivisions known of Defendants' fraudulent non-compliance, which resulted in the submission of ineligible false claims for reimbursement, they would not have paid the claims.

396. The above-named Defendants' presentment, or causation of presentment, of false and/or fraudulent claims to the State of Delaware and its political subdivisions was a foreseeable factor in the State of Delaware and its political subdivisions' loss and a consequence of Defendants' fraudulent scheme. By virtue of the above-named Defendants' actions, the State of Delaware and its political subdivisions have suffered damages.

2. Making or Using False Records or Statements Material to False and/or Fraudulent Claims (DEL. CODE ANN. § 1201(a)(2))

397. From at least 2013 to the present, the above-named Defendants knowingly made, used, or caused to be made or used, false records or statements that were material to false and/or fraudulent claims paid or approved by the State of Delaware and its political subdivisions. These false records or statements include those made on websites and in other marketing materials.

398. The above-named Defendants knowingly and fraudulently used the false statements in their marketing materials and websites both to induce the State of Delaware and its political subdivisions to enter into the contracts and agreements at issue and to get false and/or fraudulent claims made pursuant to those contracts paid or approved by the State of Delaware and its political subdivisions.

399. The above-named Defendants' false statements or records, or causation of false statements or records, had the potential to influence the State of Delaware and its political subdivisions' payment decision and were material to the State of Delaware and its political subdivisions' decision to pay the claims.

400. The above-named Defendants' false statements regarding the exclusivity and deployment models of the cloud services at issue were material because they went to the very essence of the bargain for which the State of Delaware and its political subdivisions contracted. Had the State of Delaware and its political subdivisions known of Defendants' fraudulent misrepresentations regarding the cloud services at issue, which resulted in the submission of ineligible false and/or fraudulent claims for reimbursement, then the State of Delaware and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under those contracts and agreements.

401. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the DFCA.

402. The above-named Defendants' submission, or causation of submission, of false records and statements material to false and/or fraudulent claims was a foreseeable factor in the State of Delaware's loss and a consequence of Defendants' scheme. By virtue of Defendants' actions, the State of Delaware and its political subdivisions have suffered damages.

3. Conspiracy (DEL. CODE ANN. § 1201(a)(3))

403. From at least 2013 to the present, the above-named Defendants conspired together to: (1) fraudulently induce the State of Delaware and its political subdivisions to enter into contracts and agreements with them; and (2) submit or cause the submission of false and/or

fraudulent claims under those contracts and agreements to the State of Delaware and its political subdivisions.

404. Microsoft entered into agreements with the State of Delaware and its political subdivisions that are part and parcel of Defendant SHI's contracts with the State of Delaware and its political subdivisions for the cloud services at issue.

405. Defendant SHI, having issued all invoices for the specific products at issue, knew that cloud services marketed as "for Government" which utilized Microsoft's "fake SKU" included commercial cloud services, and were therefore not actually "for Government."

406. The above-named Defendants' conspiracy had the potential to influence the State of Delaware and its political subdivisions' payment decision because State of Delaware and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under them had they known that they were not receiving true "government cloud" services.

* * *

407. WHEREFORE, Relator respectfully requests that the Court enter judgment against Defendants, and award the following:

To the STATE OF DELAWARE:

a) Three times the amount of damages that the State of Delaware has sustained as a result of Defendants' fraudulent and illegal practices;

b) Civil penalties against Defendants up to the maximum allowed by law for each violation of DEL. CODE ANN. tit. 6, § 1201(a); and

c) All costs incurred in bringing this action.

To RELATOR:

a) The maximum amount allowed pursuant to DEL. CODE ANN. tit. 6, § 1205(a) and/or any other applicable provision of law;

b) Reimbursement for reasonable expenses Relator incurred in connection with this action;

c) An award of reasonable attorney's fees and costs; and

d) Such further relief as this Court deems equitable and just.

H. Count VIII – Florida False Claims Act

408. Relator realleges and hereby incorporates by reference each and every allegation contained in all paragraphs of this complaint.

409. This is a *qui tam* action brought by Relator and the State of Florida to recover treble damages and civil penalties under the Florida False Claims Act ("FFCA"), FLA. STAT. §§ 68.081–68.092.

410. The FFCA provides that any person who:

(a) Knowingly presents or causes to be presented a false or fraudulent claim for payment or approval; [or]
(b) Knowingly makes, uses or causes to be made or used a false record or statement material to a false or fraudulent claim; [or]
(c) Conspires to commit a violation of [the FFCA];

FLA. STAT. § 68.082(2), is liable to the State of Florida for a civil penalty of $5,500 to $11,000 for each violation of the FFCA, plus three times the amount of damages which the State of Florida sustains because of the violation. *Id.*

1. Presentment of False and/or Fraudulent Claims (FLA. STAT. § 68.082(2)(a))

411. From at least 2012 to the present, the following Defendants knowingly presented, or caused to be presented, false and/or fraudulent claims to the State of Florida and its political subdivisions for payment or approval: Microsoft Corporation; Microsoft Licensing, G.P.; CDW Government, LLC; Champion Solutions Group, Inc.; Cornerstone IT, Inc.; Imager Software, Inc.; Insight Public Sector, Inc.; Planet Technologies, Inc.; and SHI International Corporation.

412. The above-named Defendants fraudulently induced the State of Florida and its political subdivisions to enter into contracts and agreements for cloud computing services by making false statements regarding the cloud services' government exclusivity and security. Defendants made these false statements in marketing and advertising materials as well as in the contracts and agreements themselves.

413. The above-named Defendants also made false certifications in the contracts and agreements at issue as to: (1) the truth, completeness, and accuracy of information provided; and (2) compliance with laws.

414. The above-named Defendants submitted claims for payment to the State of Florida and its political subdivisions under the contracts and agreements at issue, which were both fraudulently induced and/or contain false statements and certifications.

415. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the FFCA.

416. The above-named Defendants' knowing submission, or causation of submission, of false and/or fraudulent claims had the potential to influence the State of Florida and its political subdivisions' payment decision and was material to the State of Florida and its political subdivisions' decision to pay the claims.

417. The above-named Defendants' misrepresentations regarding the cloud services at issue and their compliance with the applicable standards for cloud computing are material because they went to the very essence of the bargain for which the State of Florida and its political subdivisions contracted. Had the State of Florida and its political subdivisions known of Defendants' fraudulent non-compliance, which resulted in the submission of ineligible false claims for reimbursement, they would not have paid the claims.

418. The above-named Defendants' presentment, or causation of presentment, of false and/or fraudulent claims to the State of Florida and its political subdivisions was a foreseeable factor in the State of Florida and its political subdivisions' loss and a consequence of Defendants' fraudulent scheme. By virtue of the above-named Defendants' actions, the State of Florida and its political subdivisions have suffered damages.

2. Making or Using False Records or Statements Material to False and/or Fraudulent Claims (FLA. STAT. § 68.082(2)(b))

419. From at least 2012 to the present, the above-named Defendants knowingly made, used, or caused to be made or used, false records or statements that were material to false and/or fraudulent claims paid or approved by the State of Florida and its political subdivisions. These false records or statements include those made on websites and in other marketing materials.

420. The above-named Defendants knowingly and fraudulently used the false statements in their marketing materials and websites both to induce the State of Florida and its political subdivisions to enter into the contracts and agreements at issue and to get false and/or fraudulent claims made pursuant to those contracts paid or approved by the State of Florida and its political subdivisions.

421. The above-named Defendants' false statements or records, or causation of false statements or records, had the potential to influence the State of Florida and its political subdivisions' payment decision and were material to the State of Florida and its political subdivisions' decision to pay the claims.

422. The above-named Defendants' false statements regarding the exclusivity and deployment models of the cloud services at issue were material because they went to the very essence of the bargain for which the State of Florida and its political subdivisions contracted. Had the State of Florida and its political subdivisions known of Defendants' fraudulent

misrepresentations regarding the cloud services at issue, which resulted in the submission of ineligible false and/or fraudulent claims for reimbursement, then the State of Florida and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under those contracts and agreements.

423. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the FFCA.

424. The above-named Defendants' submission, or causation of submission, of false records and statements material to false and/or fraudulent claims was a foreseeable factor in the State of Florida's loss and a consequence of Defendants' scheme. By virtue of Defendants' actions, the State of Florida and its political subdivisions have suffered damages.

3. Conspiracy (FLA. STAT. § 68.082(2)(c))

425. From at least 2012 to the present, the above-named Defendants conspired together to: (1) fraudulently induce the State of Florida and its political subdivisions to enter into contracts and agreements with them; and (2) submit or cause the submission of false and/or fraudulent claims under those contracts and agreements to the State of Florida and its political subdivisions.

426. Microsoft entered into agreements with the State of Florida and its political subdivisions that are part and parcel of the above-named Reseller Defendants' contracts with the State of Florida and its political subdivisions for the cloud services at issue.

427. The above-named Reseller Defendants, having issued all invoices for the specific products at issue, knew that cloud services marketed as "for Government" which utilized Microsoft's "fake SKU" included commercial cloud services, and were therefore not actually "for Government."

428. The above-named Defendants' conspiracy had the potential to influence the State of Florida and its political subdivisions' payment decision because State of Florida and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under them had they known that they were not receiving true "government cloud" services.

* * *

429. WHEREFORE, Relator respectfully requests that the Court enter judgment against Defendants, and award the following:

To the STATE OF FLORIDA:

a) Three times the amount of damages that the State of Florida has sustained as a result of Defendants' fraudulent and illegal practices;

b) Civil penalties against Defendants up to the maximum allowed by law for each violation of FLA. STAT. § 68.082(2); and

c) All costs incurred in bringing this action.

To RELATOR:

a) The maximum amount allowed pursuant to FLA. STAT. § 68.085 and/or any other applicable provision of law;

b) Reimbursement for reasonable expenses Relator incurred in connection with this action;

c) An award of reasonable attorney's fees and costs; and

d) Such further relief as this Court deems equitable and just.

I. Count IX – Hawaii False Claims Acts to the State

430. Relator realleges and hereby incorporates by reference each and every allegation contained in all paragraphs of this complaint.

431. This is a *qui tam* action brought by Relator and the State of Hawaii to recover treble damages and civil penalties under the Hawaii False Claims Act to the State, HAW. REV. STAT. §§ 661-21–661-31.

432. The Hawaii False Claims Act to the State provides that any person who:

> (1) Knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval; [or]
> (2) Knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim; [or] . . .
> (8) Conspires to commit any of the conduct described [above];

HAW. REV. STAT. § 661-21(a), is liable to the State of Hawaii for a civil penalty of $5,500 to $11,000 for each violation of the Hawaii False Claims Act to the State, plus three times the amount of damages which the State of Hawaii sustains due to the violation. *See id.*

1. Presentment of False and/or Fraudulent Claims (HAW. REV. STAT. § 661-21(a)(1))

433. From at least 2016 to the present, the following Defendants knowingly presented, or caused to be presented, false and/or fraudulent claims to the State of Hawaii and its political subdivisions for payment or approval: Microsoft Corporation; En Pointe Technologies Sales, LLC; Intraprise TechKnowlogies LLC; and PCM, Inc.

434. The above-named Defendants fraudulently induced the State of Hawaii and its political subdivisions to enter into contracts and agreements for cloud computing services by making false statements regarding the cloud services' government exclusivity and security. Defendants made these false statements in marketing and advertising materials and/or in the contracts and agreements themselves.

435. The above-named Defendants submitted claims for payment to the State of Hawaii and its political subdivisions under the contracts and agreements at issue, which were fraudulently induced.

436. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the Hawaii False Claims Act to the State.

437. The above-named Defendants' knowing submission, or causation of submission, of false and/or fraudulent claims had the potential to influence the State of Hawaii and its political subdivisions' payment decision and was material to the State of Hawaii and its political subdivisions' decision to pay the claims.

438. The above-named Defendants' misrepresentations regarding the cloud services at issue and their compliance with the applicable standards for cloud computing are material because they went to the very essence of the bargain for which the State of Hawaii and its political subdivisions contracted. Had the State of Hawaii and its political subdivisions known of Defendants' fraudulent non-compliance, which resulted in the submission of ineligible false claims for reimbursement, they would not have paid the claims.

439. The above-named Defendants' presentment, or causation of presentment, of false and/or fraudulent claims to the State of Hawaii and its political subdivisions was a foreseeable factor in the State of Hawaii and its political subdivisions' loss and a consequence of Defendants' fraudulent scheme. By virtue of the above-named Defendants' actions, the State of Hawaii and its political subdivisions have suffered damages.

2. Making or Using False Records or Statements Material to False and/or Fraudulent Claims (HAW. REV. STAT. § 661-21(a)(2))

440. From at least 2016 to the present, the above-named Defendants knowingly made, used, or caused to be made or used, false records or statements that were material to false and/or fraudulent claims paid or approved by the State of Hawaii and its political subdivisions. These false records or statements include those made on websites and in other marketing materials.

441. The above-named Defendants knowingly and fraudulently used the false statements in their marketing materials and websites both to induce the State of Hawaii and its political subdivisions to enter into the contracts and agreements at issue and to get false and/or fraudulent claims made pursuant to those contracts paid or approved by the State of Hawaii and its political subdivisions.

442. The above-named Defendants' false statements or records, or causation of false statements or records, had the potential to influence the State of Hawaii and its political subdivisions' payment decision and were material to the State of Hawaii and its political subdivisions' decision to pay the claims.

443. The above-named Defendants' false statements regarding the exclusivity and deployment models of the cloud services at issue were material because they went to the very essence of the bargain for which the State of Hawaii and its political subdivisions contracted. Had the State of Hawaii and its political subdivisions known of Defendants' fraudulent misrepresentations regarding the cloud services at issue, which resulted in the submission of ineligible false and/or fraudulent claims for reimbursement, then the State of Hawaii and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under those contracts and agreements.

444. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the Hawaii False Claims Act to the State.

445. The above-named Defendants' submission, or causation of submission, of false records and statements material to false and/or fraudulent claims was a foreseeable factor in the State of Hawaii's and its political subdivisions' loss and a consequence of Defendants' scheme.

By virtue of Defendants' actions, the State of Hawaii and its political subdivisions have suffered damages.

3. Conspiracy (HAW. REV. STAT. § 661-21(a)(8))

446. From 2012 to the present, the above-named Defendants conspired together to: (1) fraudulently induce the State of Hawaii and its political subdivisions to enter into contracts and agreements with them; and (2) submit or cause the submission of false and/or fraudulent claims under those contracts and agreements to the State of Hawaii and its political subdivisions.

447. Microsoft entered into agreements with the State of Hawaii and its political subdivisions that are part and parcel of the above-named Reseller Defendants' contracts with the State of Hawaii and its political subdivisions for the cloud services at issue.

448. The above-named Reseller Defendants, having issued all invoices for the specific products at issue, knew that cloud services marketed as "for Government" which utilized Microsoft's "fake SKU" included commercial cloud services, and were therefore not actually "for Government."

449. The above-named Defendants' conspiracy had the potential to influence the State of Hawaii and its political subdivisions' payment decision because State of Hawaii and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under them had they known that they were not receiving true "government cloud" services.

* * *

450. WHEREFORE, Relator respectfully requests that the Court enter judgment against Defendants, and award the following:

To the STATE OF HAWAII:

a) Three times the amount of damages that the State of Hawaii has sustained as a result of Defendants' fraudulent and illegal practices;

b) Civil penalties against Defendants up to the maximum allowed by law for each violation of HAW. REV. STAT. § 661-21; and

c) All costs incurred in bringing this action.

To RELATOR:

a) The maximum amount allowed pursuant to HAW. REV. STAT. § 661-27 and/or any other applicable provision of law;

b) Reimbursement for reasonable expenses Relator incurred in connection with this action;

c) An award of reasonable attorney's fees and costs; and

d) Such further relief as this Court deems equitable and just.

J. Count X – Hawaii False Claims Acts to the Counties

451. Relator realleges and hereby incorporates by reference each and every allegation contained in all paragraphs of this complaint.

452. This is a *qui tam* action brought by Relator, the State of Hawaii, and the Counties of Hawaii, Honolulu, and Maui, Hawaii to recover treble damages and civil penalties under the Hawaii False Claims Act to the Counties, HAW. REV. STAT. §§ 46-171–46-181.

453. The Hawaii False Claims Act to the Counties provides that any person who:

(1) Knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval; [or]
(2) Knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim; [or] . . .
(8) Conspires to commit any of the conduct described [above];

HAW. REV. STAT. § 46-171(a), is liable to the State of Hawaii for a civil penalty of $5,500 to $11,000 for each violation, plus three times the amount of damages which the State of Hawaii and its Counties sustain because of the violation. *See id.*

1. Presentment of False and/or Fraudulent Claims (HAW. REV. STAT. § 46-171(a)(1))

454. From at least 2016 to the present, the following Defendants knowingly presented, or caused to be presented, false and/or fraudulent claims to the State of Hawaii and its political subdivisions—namely, the Counties of Hawaii, Honolulu, and Maui—for payment or approval: Microsoft Corporation; En Pointe Technologies Sales, LLC; and PCM, Inc.

455. The above-named Defendants fraudulently induced the State of Hawaii and its Counties to enter into contracts and agreements for cloud computing services by making false statements regarding the cloud services' government exclusivity and security. Defendants made these false statements in marketing and advertising materials and/or in the contracts and agreements themselves.

456. The above-named Defendants submitted claims for payment to the State of Hawaii and its Counties under the contracts and agreements at issue, which were fraudulently induced.

457. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the Hawaii False Claims Act to the Counties.

458. The above-named Defendants' knowing submission, or causation of submission, of false and/or fraudulent claims had the potential to influence the State of Hawaii and its Counties' payment decision and was material to the State of Hawaii and its Counties' decision to pay the claims.

459. The above-named Defendants' misrepresentations regarding the cloud services at issue and their compliance with the applicable standards for cloud computing are material because they went to the very essence of the bargain for which the State of Hawaii and its political subdivisions contracted. Had the State of Hawaii and its Counties known of

Defendants' fraudulent non-compliance, which resulted in the submission of ineligible false claims for reimbursement, they would not have paid the claims.

460. The above-named Defendants' presentment, or causation of presentment, of false and/or fraudulent claims to the State of Hawaii and its Counties was a foreseeable factor in the State of Hawaii and its Counties' loss and a consequence of Defendants' fraudulent scheme. By virtue of the above-named Defendants' actions, the State of Hawaii and its Counties have suffered damages.

2. Making or Using False Records or Statements Material to False and/or Fraudulent Claims (HAW. REV. STAT. § 46-171(a)(2))

461. From at least 2016 to the present, the above-named Defendants knowingly made, used, or caused to be made or used, false records or statements that were material to false and/or fraudulent claims paid or approved by the State of Hawaii and its Counties. These false records or statements include those made on websites and in other marketing materials.

462. The above-named Defendants knowingly and fraudulently used the false statements in their marketing materials and websites both to induce the State of Hawaii and its Counties to enter into the contracts and agreements at issue and to get false and/or fraudulent claims made pursuant to those contracts paid or approved by the State of Hawaii and its Counties.

463. The above-named Defendants' false statements or records, or causation of false statements or records, had the potential to influence the State of Hawaii and its Counties' payment decision and were material to the State of Hawaii and its Counties' decision to pay the claims.

464. The above-named Defendants' false statements regarding the exclusivity and deployment models of the cloud services at issue were material because they went to the very

essence of the bargain for which the State of Hawaii and its Counties contracted. Had the State of Hawaii and its Counties known of Defendants' fraudulent misrepresentations regarding the cloud services at issue, which resulted in the submission of ineligible false and/or fraudulent claims for reimbursement, then the State of Hawaii and its Counties would not have entered into the contracts and agreements at issue or paid claims under those contracts and agreements.

465. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the Hawaii False Claims Act to the Counties.

466. The above-named Defendants' submission, or causation of submission, of false records and statements material to false and/or fraudulent claims was a foreseeable factor in the State of Hawaii's and its Counties' loss and a consequence of Defendants' scheme. By virtue of Defendants' actions, the State of Hawaii and its Counties have suffered damages.

3. Conspiracy (HAW. REV. STAT. § 46-171(a)(8))

467. From 2012 to the present, the above-named Defendants conspired together to: (1) fraudulently induce the State of Hawaii and its Counties to enter into contracts and agreements with them; and (2) submit or cause the submission of false and/or fraudulent claims under those contracts and agreements to the State of Hawaii and its Counties.

468. Microsoft entered into agreements with the State of Hawaii and its Counties that are part and parcel of the above-named Reseller Defendants' contracts with the State of Hawaii and its Counties for the cloud services at issue.

469. The above-named Reseller Defendants, having issued all invoices for the specific products at issue, knew that cloud services marketed as "for Government" which utilized Microsoft's "fake SKU" included commercial cloud services, and were therefore not actually "for Government."

470. The above-named Defendants' conspiracy had the potential to influence the State of Hawaii and its Counties' payment decision because State of Hawaii and its Counties would not have entered into the contracts and agreements at issue or paid claims under them had they known that they were not receiving true "government cloud" services.

* * *

471. WHEREFORE, Relator respectfully requests that the Court enter judgment against Defendants, and award the following:

To the STATE OF HAWAII and the Counties of Hawaii, Honolulu, and Maui, Hawaii:

a) Three times the amount of damages that the State of Hawaii and the Counties of Hawaii, Honolulu, and Maui have sustained as a result of Defendants' fraudulent and illegal practices;

b) Civil penalties against Defendants up to the maximum allowed by law for each violation of HAW. REV. STAT. § 46-171(a); and

c) All costs incurred in bringing this action.

To RELATOR:

a) The maximum amount allowed pursuant to HAW. REV. STAT. § 46-177 and/or any other applicable provision of law;

b) Reimbursement for reasonable expenses Relator incurred in connection with this action;

c) An award of reasonable attorney's fees and costs; and

d) Such further relief as this Court deems equitable and just.

K. Count XI – Illinois False Claims Act

472. Relator realleges and hereby incorporates by reference each and every allegation contained in all paragraphs of this complaint.

473. This is a *qui tam* action brought by Relator and the State of Illinois to recover treble damages and civil penalties under the Illinois False Claims Act ("Illinois FCA"), 740 ILL. COMP. STAT. §§ 175/1–175/8.

474. The Illinois FCA provides that any person who:

> (A) Knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval; [or]
> (B) Knowingly makes, uses or causes to be made or used a false record or statement material to a false or fraudulent claim; [or]
> (C) Conspires to commit a violation of [the above paragraphs];

740 ILL. COMP. STAT. § 175/3(a)(1), is liable to the State of Illinois for a civil penalty of $11,181 to $22,363 for each violation of the Illinois FCA, plus three times the amount of damages which the State of Illinois sustains because of the violation. *See* 28 C.F.R. § 85.5; 740 ILL. COMP. STAT. § 175/3(a)(1).

1. Presentment of False and/or Fraudulent Claims (740 ILL. COMP. STAT. § 175/3(a)(1)(A))

475. From 2012 to the present, the following Defendants knowingly presented, or caused to be presented, false and/or fraudulent claims to the State of Illinois and its political subdivisions: Microsoft Corporation; Microsoft Licensing, G.P.; and CDW Government, LLC.

476. The above-named Defendants fraudulently induced the State of Illinois and its political subdivisions to enter into contracts and agreements for cloud computing services by making false statements regarding the cloud services' government exclusivity and security. Defendants made these false statements in marketing and advertising materials as well as in the contracts and agreements themselves.

477. The above-named Defendants also made false certifications in the contracts and agreements at issue as to compliance with applicable laws.

478. The above-named Defendants submitted claims for payment to the State of Illinois and its political subdivisions under the contracts and agreements at issue, which were both fraudulently induced and/or contain false statements and certifications.

479. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the Illinois FCA.

480. The above-named Defendants' knowing submission, or causation of submission, of false and/or fraudulent claims had the potential to influence the State of Illinois and its political subdivisions' payment decision and was material to the State of Illinois' and its political subdivisions' decision to pay the claims.

481. The above-named Defendants' misrepresentations regarding the cloud services at issue and their compliance with the applicable standards for cloud computing are material because they went to the very essence of the bargain for which the State of Illinois and its political subdivisions contracted. Had the State of Illinois and its political subdivisions known of Defendants' fraudulent non-compliance, which resulted in the submission of ineligible false claims for reimbursement, they would not have paid the claims.

482. The above-named Defendants' presentment, or causation of presentment, of false and/or fraudulent claims to the State of Illinois and its political subdivisions was a foreseeable factor in the State of Illinois and its political subdivisions' loss and a consequence of Defendants' fraudulent scheme. By virtue of the above-named Defendants' actions, the State of Illinois and its political subdivisions have suffered damages.

2. Making or Using False Records or Statements Material to False and/or Fraudulent Claims (740 ILL. COMP. STAT. § 175/3(a)(1)(B))

483. From 2012 to the present, the above-named Defendants knowingly made, used, or caused to be made or used, false records or statements that were material to false and/or

fraudulent claims paid or approved by the State of Illinois and its political subdivisions. These false records or statements include those made on websites and in other marketing materials.

484. The above-named Defendants knowingly and fraudulently used the false statements in their marketing materials and websites both to induce the State of Illinois and its political subdivisions to enter into the contracts and agreements at issue and to get false and/or fraudulent claims made pursuant to those contracts paid or approved by the State of Illinois and its political subdivisions.

485. The above-named Defendants' false statements or records, or causation of false statements or records, had the potential to influence the State of Illinois and its political subdivisions' payment decision and were material to the State of Illinois and its political subdivisions' decision to pay the claims.

486. The above-named Defendants' false statements regarding the exclusivity and deployment models of the cloud services at issue were material because they went to the very essence of the bargain for which the State of Illinois and its political subdivisions contracted. Had the State of Illinois and its political subdivisions known of Defendants' fraudulent misrepresentations regarding the cloud services at issue, which resulted in the submission of ineligible false and/or fraudulent claims for reimbursement, then the State of Illinois and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under those contracts and agreements.

487. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the Illinois FCA.

488. The above-named Defendants' submission, or causation of submission, of false records and statements material to false and/or fraudulent claims was a foreseeable factor in the

State of Illinois' loss and a consequence of Defendants' scheme. By virtue of Defendants' actions, the State of Illinois and its political subdivisions have suffered damages.

3. Conspiracy (740 ILL. COMP. STAT. § 175/3(a)(1)(C))

489. From 2012 to the present, the above-named Defendants conspired together to: (1) fraudulently induce the State of Illinois and its political subdivisions to enter into contracts and agreements with them; and (2) submit or cause the submission of false and/or fraudulent claims under those contracts and agreements to the State of Illinois and its political subdivisions.

490. Microsoft entered into agreements with the State of Illinois and its political subdivisions that are part and parcel of CDW Government, LLC's contracts with the State of Illinois and its political subdivisions for the cloud services at issue.

491. Defendant CDW Government, LLC, having issued all invoices for the specific products at issue, knew that cloud services marketed as "for Government" which utilized Microsoft's "fake SKU" included commercial cloud services, and were therefore not actually "for Government."

492. The above-named Defendants' conspiracy had the potential to influence the State of Illinois and its political subdivisions' payment decision because State of Illinois and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under them had they known that they were not receiving true "government cloud" services.

* * *

493. WHEREFORE, Relator respectfully requests that the Court enter judgment against Defendants, and award the following:

To the STATE OF ILLINOIS:

a) Three times the amount of damages that the State of Illinois has sustained as a result of Defendants' fraudulent and illegal practices;

b) Civil penalties against Defendants up to the maximum allowed by law for each violation of 740 ILL. COMP. STAT. § 175/3(a)(1); and

c) All costs incurred in bringing this action.

To RELATOR:

a) The maximum amount allowed pursuant to 740 ILL. COMP. STAT. § 175/4(d) and/or any other applicable provision of law;

b) Reimbursement for reasonable expenses Relator incurred in connection with this action;

c) An award of reasonable attorney's fees and costs; and

d) Such further relief as this Court deems equitable and just.

L. Count XII – Indiana False Claims and Whistleblower Protection Act

494. Relator realleges and hereby incorporates by reference each and every allegation contained in all paragraphs of this complaint.

495. This is a *qui tam* action brought by Relator and the State of Indiana to recover treble damages and civil penalties under the Indiana False Claims and Whistleblower Protection Act ("Indiana FCA"), IND. CODE §§ 5-11-5.5-1–5-11-5.5-18.

496. The Indiana FCA provides that any person who knowingly or intentionally:

(1) presents a false claim to the state for payment or approval; [or]
(2) makes or uses a false record or statement to obtain payment or approval of a false claim from the state; [or] . . .
(8) conspires with another person to perform an act described [above,]

IND. CODE § 5-11-5.5-2(b), is liable to the State of Indiana for a civil penalty of at least $5,000 for each violation of the Indiana FCA, plus three times the amount of damages which the State of Indiana sustains because of the violation. *See id.*

1. Presentment of False Claims (IND. CODE. § 5-11-5.5-2(b)(1))

497. From at least 2014 to the present, the following Defendants knowingly or intentionally presented false claims to the State of Indiana and its political subdivisions for payment or approval: Microsoft Corporation; CDW Corporation; and Dell Marketing, L.P..

498. The above-named Defendants fraudulently induced the State of Indiana and its political subdivisions to enter into contracts and agreements for cloud computing services by making false statements regarding the cloud services' government exclusivity and security. Defendants made these false statements in marketing and advertising materials and in the contracts and agreements themselves.

499. The above-named Defendants submitted claims for payment to the State of Indiana and its political subdivisions under the contracts and agreements at issue, which were fraudulently induced.

500. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the Indiana FCA.

501. The above-named Defendants' knowing or intentional submission of false claims had the potential to influence the State of Indiana and its political subdivisions' payment decision and was material to the State of Indiana and its political subdivisions' decision to pay the claims.

502. The above-named Defendants' misrepresentations regarding the cloud services at issue and their compliance with the applicable standards for cloud computing are material because they went to the very essence of the bargain for which the State of Indiana and its political subdivisions contracted. Had the State of Indiana and its political subdivisions known of Defendants' fraudulent non-compliance, which resulted in the submission of ineligible false claims for reimbursement, they would not have paid the claims.

503. The above-named Defendants' presentment, or causation of presentment, of false and/or fraudulent claims to the State of Indiana and its political subdivisions was a foreseeable factor in the State of Indiana and its political subdivisions' loss and a consequence of Defendants' fraudulent scheme. By virtue of the above-named Defendants' actions, the State of Indiana and its political subdivisions have suffered damages.

2. Making or Using False Records or Statements to Obtain Payment or Approval of False Claims (IND. CODE § 5-11-5.5-2(b)(2))

504. From at least 2014 to the present, the above-named Defendants knowingly made or used false records or statements to get false claims paid or approved by the State of Indiana and its political subdivisions. These false records or statements include those made on websites and in other marketing materials.

505. The above-named Defendants knowingly and fraudulently used the false statements in their marketing materials and websites both to induce the State of Indiana and its political subdivisions to enter into the contracts and agreements at issue and to get false claims made pursuant to those contracts paid or approved by the State of Indiana and its political subdivisions.

506. The above-named Defendants' false statements or records, or causation of false statements or records, had the potential to influence the State of Indiana and its political subdivisions' payment decision and were material to the State of Indiana and its political subdivisions' decision to pay the claims.

507. The above-named Defendants' false statements regarding the exclusivity and deployment models of the cloud services at issue were material because they went to the very essence of the bargain for which the State of Indiana and its political subdivisions contracted. Had the State of Indiana and its political subdivisions known of Defendants' fraudulent

misrepresentations regarding the cloud services at issue, which resulted in the submission of ineligible false claims for reimbursement, then the State of Indiana and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under those contracts and agreements.

508. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the Indiana FCA.

509. The above-named Defendants' use or creation of false records and statements was a foreseeable factor in the State of Indiana's and its political subdivisions' loss and a consequence of Defendants' scheme. By virtue of Defendants' actions, the State of Indiana and its political subdivisions have suffered damages.

3. Conspiracy (IND. CODE § 5-11-5.5-2(b)(8))

510. From at least 2014 to the present, the above-named Defendants conspired together to: (1) fraudulently induce the State of Indiana and its political subdivisions to enter into contracts and agreements with them; and (2) submit or cause the submission of false claims under those contracts and agreements to the State of Indiana and its political subdivisions.

511. Microsoft entered into agreements with the State of Indiana and its political subdivisions that are part and parcel of the above-named Reseller Defendants' contracts with the State of Indiana and its political subdivisions for the cloud services at issue.

512. The above-named Reseller Defendants, having issued all invoices for the specific products at issue, knew that cloud services marketed as "for Government" which utilized Microsoft's "fake SKU" included commercial cloud services, and were therefore not actually "for Government."

513. The above-named Defendants' conspiracy had the potential to influence the State of Indiana and its political subdivisions' payment decision because State of Indiana and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under them had they known that they were not receiving true "government cloud" services.

* * *

514. WHEREFORE, Relator respectfully requests that the Court enter judgment against Defendants, and award the following:

To the STATE OF INDIANA

a) Three times the amount of damages that the State of Indiana has sustained as a result of Defendants' fraudulent and illegal practices;

b) Civil penalties against Defendants up to the maximum allowed by law for each violation of IND. CODE § 5-11-5.5-2(a); and

c) All costs incurred in bringing this action.

To RELATOR:

a) The maximum amount allowed pursuant to IND. CODE § 5-11-5.5-6 and/or any other applicable provision of law;

b) Reimbursement for reasonable expenses Relator incurred in connection with this action;

c) An award of reasonable attorney's fees and costs; and

d) Such further relief as this Court deems equitable and just.

M. Count XIII – Iowa False Claims Act

515. Relator realleges and hereby incorporates by reference each and every allegation contained in all paragraphs of this complaint.

516. This is a *qui tam* action brought by Relator and the State of Iowa to recover treble damages and civil penalties under the Iowa False Claims Act ("Iowa FCA"), IOWA CODE §§ 685.1–685.7.

517. The Iowa FCA provides that any person who:

> (a) Knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval; [or]
> (b) Knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim; [or]
> (c) Conspires to commit a violation of [the above paragraphs,]

IOWA CODE § 685.2(1), is liable to the State of Iowa for a civil penalty of $11,181 to $22,363 for each violation of the Iowa FCA, plus three times the amount of damages which the State of Iowa sustains because of the violation. *See* 28 C.F.R. § 85.5; IOWA CODE § 685.2(1).

1. Presentment of False and/or Fraudulent Claims (IOWA CODE § 685.2(1)(a))

518. From at least 2016 to the present, Defendants Microsoft Corporation and Insight Public Sector, Inc. knowingly presented, or caused to be presented, false and/or fraudulent claims to the State of Iowa and its political subdivisions for payment or approval.

519. The above-named Defendants fraudulently induced the State of Iowa and its political subdivisions to enter into contracts and agreements for cloud computing services by making false statements regarding the cloud services' government exclusivity and security. Defendants made these false statements in marketing and advertising materials as well as in the contracts and agreements themselves.

520. The above-named Defendants also made false certifications in the contracts and agreements at issue as to compliance with applicable laws.

521. The above-named Defendants submitted claims for payment to the State of Iowa and its political subdivisions under the contracts and agreements at issue, which were both fraudulently induced and/or contain false statements and certifications.

522. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the Iowa FCA.

523. The above-named Defendants' knowing submission, or causation of submission, of false and/or fraudulent claims had the potential to influence the State of Iowa and its political subdivisions' payment decision and was material to the State of Iowa's and its political subdivisions' decision to pay the claims.

524. The above-named Defendants' misrepresentations regarding the cloud services at issue and their compliance with the applicable standards for cloud computing are material because they went to the very essence of the bargain for which the State of Iowa and its political subdivisions contracted. Had the State of Iowa and its political subdivisions known of Defendants' fraudulent non-compliance, which resulted in the submission of ineligible false claims for reimbursement, they would not have paid the claims.

525. The above-named Defendants' presentment, or causation of presentment, of false and/or fraudulent claims to the State of Iowa and its political subdivisions was a foreseeable factor in the State of Iowa and its political subdivisions' loss and a consequence of Defendants' fraudulent scheme. By virtue of the above-named Defendants' actions, the State of Iowa and its political subdivisions have suffered damages.

2. Making or Using False Records or Statements Material to False and/or Fraudulent Claims (IOWA CODE § 685.2(1)(b))

526. From at least 2016 to the present, the above-named Defendants knowingly made, used, or caused to be made or used, false records or statements that were material to false and/or

fraudulent claims paid or approved by the State of Iowa and its political subdivisions. These false records or statements include those made on websites and in other marketing materials.

527. The above-named Defendants knowingly and fraudulently used the false statements in their marketing materials and websites both to induce the State of Iowa and its political subdivisions to enter into the contracts and agreements at issue and to get false and/or fraudulent claims made pursuant to those contracts paid or approved by the State of Iowa and its political subdivisions.

528. The above-named Defendants' false statements or records, or causation of false statements or records, had the potential to influence the State of Iowa and its political subdivisions' payment decision and were material to the State of Iowa and its political subdivisions' decision to pay the claims.

529. The above-named Defendants' false statements regarding the exclusivity and deployment models of the cloud services at issue were material because they went to the very essence of the bargain for which the State of Iowa and its political subdivisions contracted. Had the State of Iowa and its political subdivisions known of Defendants' fraudulent misrepresentations regarding the cloud services at issue, which resulted in the submission of ineligible false and/or fraudulent claims for reimbursement, then the State of Iowa and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under those contracts and agreements.

530. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the Iowa FCA.

531. The above-named Defendants' submission, or causation of submission, of false records and statements material to false and/or fraudulent claims was a foreseeable factor in the

State of Iowa's loss and a consequence of Defendants' scheme. By virtue of Defendants' actions, the State of Iowa and its political subdivisions have suffered damages.

3. Conspiracy (IOWA CODE § 685.2(1)(c))

532. From at least 2016 to the present, the above-named Defendants conspired together to: (1) fraudulently induce the State of Iowa and its political subdivisions to enter into contracts and agreements with them; and (2) submit or cause the submission of false and/or fraudulent claims under those contracts and agreements to the State of Iowa and its political subdivisions.

533. Microsoft entered into agreements with the State of Iowa and its political subdivisions that are part and parcel of Insight Public Sector, Inc.'s contracts with the State of Iowa and its political subdivisions for the cloud services at issue.

534. Defendant Insight Public Sector, Inc., having issued all invoices for the specific products at issue, knew that cloud services marketed as "for Government" which utilized Microsoft's "fake SKU" included commercial cloud services, and were therefore not actually "for Government."

535. The above-named Defendants' conspiracy had the potential to influence the State of Iowa and its political subdivisions' payment decision because State of Iowa and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under them had they known that they were not receiving true "government cloud" services.

* * *

536. WHEREFORE, Relator respectfully requests that the Court enter judgment against Defendants, and award the following:

To the STATE OF IOWA:

a) Three times the amount of damages that the State of Iowa has sustained as a result of Defendants' fraudulent and illegal practices;

b) Civil penalties against Defendants up to the maximum allowed by law for each violation of IOWA CODE § 685.2(1); and

c) All costs incurred in bringing this action.

To RELATOR:

a) The maximum amount allowed pursuant to IOWA CODE § 685.3(4) and/or any other applicable provision of law;

b) Reimbursement for reasonable expenses Relator incurred in connection with this action;

c) An award of reasonable attorney's fees and costs; and

d) Such further relief as this Court deems equitable and just.

N. Count XIV – Massachusetts False Claims Act

537. Relator realleges and hereby incorporates by reference each and every allegation contained in all paragraphs of this complaint.

538. This is a *qui tam* action brought by Relator and the Commonwealth of Massachusetts to recover treble damages and civil penalties under the Massachusetts False Claims Act ("MAFCA"), MASS. GEN. LAWS ANN. ch. 12, §§ 5A–5O.

539. The MAFCA provides that any person who:

(1) knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval; [or]
(2) knowingly makes, uses or causes to be made or used a false record or statement material to a false or fraudulent claim; [or]
(3) conspires to commit a violation of [the above paragraphs]; [or] . . .
(8) enters into an agreement, contract or understanding with an official of the commonwealth or a political subdivision thereof knowing the information contained therein is false[,]

MASS. GEN. LAWS ANN. ch. 12, § 5B(a), is liable to the Commonwealth of Massachusetts for a civil penalty of $11,181 to $22,363 for each violation of the MAFCA, plus three times the

amount of damages which the Commonwealth of Massachusetts sustains because of the violation. *See* 28 C.F.R. § 85.5; MASS. GEN. LAWS ANN. ch. 12, § 5B(a).

1. Presentment of False and/or Fraudulent Claims (MASS. GEN. LAWS ANN. ch. 12, § 5B(a)(1))

540. From at least 2015 to the present, the following Defendants knowingly presented, or caused to be presented, false and/or fraudulent claims to the Commonwealth of Massachusetts and its political subdivisions for payment or approval: Microsoft Corporation; CDW Government, LLC; Dell Marketing, L.P.; and SHI International Corporation.

541. The above-named Defendants fraudulently induced the Commonwealth of Massachusetts and its political subdivisions to enter into contracts and agreements for cloud computing services by making false statements regarding the cloud services' government exclusivity and security. Defendants made these false statements in marketing and advertising materials as well as in the contracts and agreements themselves.

542. The above-named Defendants submitted claims for payment to the Commonwealth of Massachusetts and its political subdivisions under the contracts and agreements at issue, which were both fraudulently induced and/or contain false statements and certifications.

543. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the MAFCA.

544. The above-named Defendants' knowing submission, or causation of submission, of false and/or fraudulent claims had the potential to influence the Commonwealth of Massachusetts and its political subdivisions' payment decision and was material to the Commonwealth of Massachusetts' and its political subdivisions' decision to pay the claims.

545. The above-named Defendants' misrepresentations regarding the cloud services at issue and their compliance with the applicable standards for cloud computing are material because they went to the very essence of the bargain for which the Commonwealth of Massachusetts and its political subdivisions contracted. Had the Commonwealth of Massachusetts and its political subdivisions known of Defendants' fraudulent non-compliance, which resulted in the submission of ineligible false claims for reimbursement, they would not have paid the claims.

546. The above-named Defendants' presentment, or causation of presentment, of false and/or fraudulent claims to the Commonwealth of Massachusetts and its political subdivisions was a foreseeable factor in the Commonwealth of Massachusetts and its political subdivisions' loss and a consequence of Defendants' fraudulent scheme. By virtue of the above-named Defendants' actions, the Commonwealth of Massachusetts and its political subdivisions have suffered damages.

2. Making or Using False Records or Statements Material to False and/or Fraudulent Claims (MASS. GEN. LAWS ANN. ch. 12, § 5B(a)(2))

547. From at least 2015 to the present, the above-named Defendants knowingly made, used, or caused to be made or used, false records or statements that were material to false and/or fraudulent claims paid or approved by the Commonwealth of Massachusetts and its political subdivisions. These false records or statements include those made on websites and in other marketing materials.

548. The above-named Defendants knowingly and fraudulently used the false statements in their marketing materials and websites both to induce the Commonwealth of Massachusetts and its political subdivisions to enter into the contracts and agreements at issue

and to get false and/or fraudulent claims made pursuant to those contracts paid or approved by the Commonwealth of Massachusetts and its political subdivisions.

549. The above-named Defendants' false statements or records, or causation of false statements or records, had the potential to influence the Commonwealth of Massachusetts and its political subdivisions' payment decision and were material to the Commonwealth of Massachusetts and its political subdivisions' decision to pay the claims.

550. The above-named Defendants' false statements regarding the exclusivity and deployment models of the cloud services at issue were material because they went to the very essence of the bargain for which the Commonwealth of Massachusetts and its political subdivisions contracted. Had the Commonwealth of Massachusetts and its political subdivisions known of Defendants' fraudulent misrepresentations regarding the cloud services at issue, which resulted in the submission of ineligible false and/or fraudulent claims for reimbursement, then the Commonwealth of Massachusetts and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under those contracts and agreements.

551. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the MAFCA.

552. The above-named Defendants' submission, or causation of submission, of false records and statements material to false and/or fraudulent claims was a foreseeable factor in the Commonwealth of Massachusetts' loss and a consequence of Defendants' scheme. By virtue of Defendants' actions, the Commonwealth of Massachusetts and its political subdivisions have suffered damages.

3. Conspiracy (MASS. GEN. LAWS ANN. ch. 12, § 5B(a)(3))

553. From at least 2015 to the present, the above-named Defendants conspired together to: (1) fraudulently induce the Commonwealth of Massachusetts and its political subdivisions to enter into contracts and agreements with them; and (2) submit or cause the submission of false and/or fraudulent claims under those contracts and agreements to the Commonwealth of Massachusetts and its political subdivisions.

554. Microsoft entered into agreements with the Commonwealth of Massachusetts and its political subdivisions that are part and parcel of the above-named Reseller Defendants' contracts with the Commonwealth of Massachusetts and its political subdivisions for the cloud services at issue.

555. The above-named Reseller Defendants, having issued all invoices for the specific products at issue, knew that cloud services marketed as "for Government" which utilized Microsoft's "fake SKU" included commercial cloud services, and were therefore not actually "for Government."

556. The above-named Defendants' conspiracy had the potential to influence the Commonwealth of Massachusetts and its political subdivisions' payment decision because the Commonwealth of Massachusetts and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under them had they known that they were not receiving true "government cloud" services.

4. False Contracts/Agreements (MASS. GEN. LAWS ANN. ch. 12, § 5B(a)(8))

557. From at least 2015 to the present, the above-named Defendants entered into agreements and contracts with the Commonwealth of Massachusetts and its political subdivisions, knowing that information contained therein was false.

558. The contracts and agreements at issue contained false certifications as to Defendants' compliance with applicable laws, and false statements regarding GCC's government exclusivity.

* * *

559. WHEREFORE, Relator respectfully requests that the Court enter judgment against Defendants, and award the following:

To the COMMONWEALTH OF MASSACHUSETTS:

a) Three times the amount of damages that the Commonwealth of Massachusetts has sustained as a result of Defendants' fraudulent and illegal practices;

b) Civil penalties against Defendants up to the maximum allowed by law for each violation of MASS. GEN. LAWS ANN. ch. 12 § 5B; and

c) All costs incurred in bringing this action.

To RELATOR:

a) The maximum amount allowed pursuant to MASS. GEN. LAWS ANN. ch. 12 § 5F and/or any other applicable provision of law;

b) Reimbursement for reasonable expenses Relator incurred in connection with this action;

c) An award of reasonable attorney's fees and costs; and

d) Such further relief as this Court deems equitable and just.

O. Count XV – Minnesota False Claims Act

560. Relator realleges and hereby incorporates by reference each and every allegation contained in all paragraphs of this complaint.

561. This is a *qui tam* action brought by Relator and the State of Minnesota to recover treble damages and civil penalties under the Minnesota False Claims Act ("MNFCA"), MINN. STAT. ANN. §§ 15C.01–15C.16.

562. The MNFCA provides that any person who:

> (1) knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval; [or]
> (2) knowingly makes or uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim; [or]
> (3) knowingly conspires to commit a violation of [the above paragraphs,]

MINN. STAT. ANN. § 15C.02(a), is liable to the State of Minnesota for a civil penalty of $5,500 to $11,000 for each violation of the MNFCA, plus three times the amount of damages which the State of Minnesota sustains because of the violation. *See id.*

1. Presentment of False and/or Fraudulent Claims (MINN. STAT. ANN. § 15C.02(a)(1))

563. From at least 2015 to the present, the following Defendants knowingly presented, or caused to be presented, false and/or fraudulent claims to the State of Minnesota and its political subdivisions for payment or approval: Microsoft Corporation; CDW Corporation; CDW Government, LLC; PCM, Inc.; PCMG, Inc.; SHI International Corporation; and T4 Technologies, Inc.

564. The above-named Defendants fraudulently induced the State of Minnesota and its political subdivisions to enter into contracts and agreements for cloud computing services by making false statements regarding the cloud services' government exclusivity and security. Defendants made these false statements in marketing and advertising materials as well as in the contracts and agreements themselves.

565. The above-named Defendants submitted claims for payment to the State of Minnesota and its political subdivisions under the contracts and agreements at issue, which were both fraudulently induced and/or contain false statements and certifications.

566. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the MNFCA.

567. The above-named Defendants' knowing submission, or causation of submission, of false and/or fraudulent claims had the potential to influence the State of Minnesota and its political subdivisions' payment decision and was material to the State of Minnesota and its political subdivisions' decision to pay the claims.

568. The above-named Defendants' misrepresentations regarding the cloud services at issue and their compliance with the applicable standards for cloud computing are material because they went to the very essence of the bargain for which the State of Minnesota and its political subdivisions contracted. Had the State of Minnesota and its political subdivisions known of Defendants' fraudulent non-compliance, which resulted in the submission of ineligible false claims for reimbursement, they would not have paid the claims.

569. The above-named Defendants' presentment, or causation of presentment, of false and/or fraudulent claims to the State of Minnesota and its political subdivisions was a foreseeable factor in the State of Minnesota and its political subdivisions' loss and a consequence of Defendants' fraudulent scheme. By virtue of the above-named Defendants' actions, the State of Minnesota and its political subdivisions have suffered damages.

2. Making or Using False Records or Statements Material to False and/or Fraudulent Claims (MINN. STAT. ANN. § 15C.02(a)(2))

570. From at least 2015 to the present, the above-named Defendants knowingly made, used, or caused to be made or used, false records or statements that were material to false and/or fraudulent claims paid or approved by the State of Minnesota and its political subdivisions. These false records or statements include those made on websites and in other marketing materials.

571. The above-named Defendants knowingly and fraudulently used the false statements in their marketing materials and websites both to induce the State of Minnesota and

its political subdivisions to enter into the contracts and agreements at issue and to get false and/or fraudulent claims made pursuant to those contracts paid or approved by the State of Minnesota and its political subdivisions.

572. The above-named Defendants' false statements or records, or causation of false statements or records, had the potential to influence the State of Minnesota and its political subdivisions' payment decision and were material to the State of Minnesota and its political subdivisions' decision to pay the claims.

573. The above-named Defendants' false statements regarding the exclusivity and deployment models of the cloud services at issue were material because they went to the very essence of the bargain for which the State of Minnesota and its political subdivisions contracted. Had the State of Minnesota and its political subdivisions known of Defendants' fraudulent misrepresentations regarding the cloud services at issue, which resulted in the submission of ineligible false and/or fraudulent claims for reimbursement, then the State of Minnesota and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under those contracts and agreements.

574. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the MNFCA.

575. The above-named Defendants' submission, or causation of submission, of false records and statements material to false and/or fraudulent claims was a foreseeable factor in the State of Minnesota's loss and a consequence of Defendants' scheme. By virtue of Defendants' actions, the State of Minnesota and its political subdivisions have suffered damages.

3. Conspiracy (MINN. STAT. ANN. § 15C.02(a)(3))

576. From at least 2015 to the present, the above-named Defendants conspired together to: (1) fraudulently induce the State of Minnesota and its political subdivisions to enter into contracts and agreements with them; and (2) submit or cause the submission of false and/or fraudulent claims under those contracts and agreements to the State of Minnesota and its political subdivisions.

577. Microsoft entered into agreements with the State of Minnesota and its political subdivisions that are part and parcel of the above-named Reseller Defendants' contracts with the State of Minnesota and its political subdivisions for the cloud services at issue.

578. The above-named Reseller Defendants, having issued all invoices for the specific products at issue, knew that cloud services marketed as "for Government" which utilized Microsoft's "fake SKU" included commercial cloud services, and were therefore not actually "for Government."

579. The above-named Defendants' conspiracy had the potential to influence the State of Minnesota and its political subdivisions' payment decision because the State of Minnesota and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under them had they known that they were not receiving true "government cloud" services.

* * *

580. WHEREFORE, Relator respectfully requests that the Court enter judgment against Defendants, and award the following:

To the STATE OF MINNESOTA:

a) Three times the amount of damages that the State of Minnesota has sustained as a result of Defendants' fraudulent and illegal practices;

b) Civil penalties against Defendants up to the maximum allowed by law for each violation of MINN. STAT. ANN. § 15C.02(a); and

c) All costs incurred in bringing this action.

To RELATOR:

a) The maximum amount allowed pursuant to MINN. STAT. ANN. § 15C.13 and/or any other applicable provision of law;

b) Reimbursement for reasonable expenses Relator incurred in connection with this action;

c) An award of reasonable attorney's fees and costs; and

d) Such further relief as this Court deems equitable and just.

P. Count XVI – Montana False Claims Act

581. Relator realleges and hereby incorporates by reference each and every allegation contained in all paragraphs of this complaint.

582. This is a *qui tam* action brought by Relator and the State of Montana to recover treble damages and civil penalties under the Montana False Claims and Reporting Act ("Montana FCA"), MONT. CODE ANN. §§ 17-8-401–17-8-416.

583. The Montana FCA provides that any person who:

(a) Knowingly presents or causes to be presented a false or fraudulent claim for payment or approval; [or]
(b) Knowingly makes, uses, or causes to be made or used a false record or statement material to a false or fraudulent claim; [or]
(c) Conspires to commit a violation of [the above paragraphs,]

MONT. CODE ANN. § 17-8-403(1), is liable to the State of Montana for a civil penalty of $11,181 to $22,363 for each violation of the Montana FCA, plus three times the amount of damages which the State of Montana sustains because of the violation. *See* 28 C.F.R. § 85.5; MONT. CODE ANN. § 1201(1), (8).

1. Presentment of False and/or Fraudulent Claims (MONT. CODE ANN. § 17-8-403(1)(a))

584. From at least 2015 to the present, the following Defendants knowingly presented, or caused to be presented, false and/or fraudulent claims to the State of Montana and its political subdivisions for payment or approval: Microsoft Corporation; Dell Marketing, L.P.; and SHI International Corporation.

585. The above-named Defendants fraudulently induced the State of Montana and its political subdivisions to enter into contracts and agreements for cloud computing services by making false statements regarding the cloud services' government exclusivity and security. Defendants made these false statements in marketing and advertising materials as well as in the contracts and agreements themselves.

586. The above-named Defendants submitted claims for payment to the State of Montana and its political subdivisions under the contracts and agreements at issue, which were both fraudulently induced and/or contain false statements and certifications.

587. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the Montana FCA.

588. The above-named Defendants' knowing submission, or causation of submission, of false and/or fraudulent claims had the potential to influence the State of Montana and its political subdivisions' payment decision and was material to the State of Montana and its political subdivisions' decision to pay the claims.

589. The above-named Defendants' misrepresentations regarding the cloud services at issue and their compliance with the applicable standards for cloud computing are material because they went to the very essence of the bargain for which the State of Montana and its political subdivisions contracted. Had the State of Montana and its political subdivisions known

of Defendants' fraudulent non-compliance, which resulted in the submission of ineligible false claims for reimbursement, they would not have paid the claims.

590. The above-named Defendants' presentment, or causation of presentment, of false and/or fraudulent claims to the State of Montana and its political subdivisions was a foreseeable factor in the State of Montana and its political subdivisions' loss and a consequence of Defendants' fraudulent scheme. By virtue of the above-named Defendants' actions, the State of Montana and its political subdivisions have suffered damages.

2. Making or Using False Records or Statements Material to False and/or Fraudulent Claims (MONT. CODE ANN. § 17-8-403(1)(b))

591. From at least 2015 to the present, the above-named Defendants knowingly made, used, or caused to be made or used, false records or statements that were material to false and/or fraudulent claims paid or approved by the State of Montana and its political subdivisions. These false records or statements include those made on websites and in other marketing materials.

592. The above-named Defendants knowingly and fraudulently used the false statements in their marketing materials and websites both to induce the State of Montana and its political subdivisions to enter into the contracts and agreements at issue and to get false and/or fraudulent claims made pursuant to those contracts paid or approved by the State of Montana and its political subdivisions.

593. The above-named Defendants' false statements or records, or causation of false statements or records, had the potential to influence the State of Montana and its political subdivisions' payment decision and were material to the State of Montana and its political subdivisions' decision to pay the claims.

594. The above-named Defendants' false statements regarding the exclusivity and deployment models of the cloud services at issue were material because they went to the very

essence of the bargain for which the State of Montana and its political subdivisions contracted. Had the State of Montana and its political subdivisions known of Defendants' fraudulent misrepresentations regarding the cloud services at issue, which resulted in the submission of ineligible false and/or fraudulent claims for reimbursement, then the State of Montana and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under those contracts and agreements.

595. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the Montana FCA.

596. The above-named Defendants' submission, or causation of submission, of false records and statements material to false and/or fraudulent claims was a foreseeable factor in the State of Montana's loss and a consequence of Defendants' scheme. By virtue of Defendants' actions, the State of Montana and its political subdivisions have suffered damages.

3. Conspiracy (MONT. CODE ANN. § 17-8-403(1)(c))

597. From at least 2015 to the present, the above-named Defendants conspired together to: (1) fraudulently induce the State of Montana and its political subdivisions to enter into contracts and agreements with them; and (2) submit or cause the submission of false and/or fraudulent claims under those contracts and agreements to the State of Montana and its political subdivisions.

598. Microsoft entered into agreements with the State of Montana and its political subdivisions that are part and parcel of the above-named Reseller Defendants' contracts with the State of Montana and its political subdivisions for the cloud services at issue.

599. The above-named Reseller Defendants, having issued all invoices for the specific products at issue, knew that cloud services marketed as "for Government" which utilized

Microsoft's "fake SKU" included commercial cloud services, and were therefore not actually "for Government."

600. The above-named Defendants' conspiracy had the potential to influence the State of Montana and its political subdivisions' payment decision because the State of Montana and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under them had they known that they were not receiving true "government cloud" services.

* * *

601. WHEREFORE, Relator respectfully requests that the Court enter judgment against Defendants, and award the following:

To the STATE OF MONTANA:

a) Three times the amount of damages that the State of Montana has sustained as a result of Defendants' fraudulent and illegal practices;

b) Civil penalties against Defendants up to the maximum allowed by law for each violation of MONT. CODE ANN. § 17-8-403(1); and

c) All costs incurred in bringing this action.

To RELATOR:

a) The maximum amount allowed pursuant to MONT. CODE ANN. § 17-8-410 and/or any other applicable provision of law;

b) Reimbursement for reasonable expenses Relator incurred in connection with this action;

c) An award of reasonable attorney's fees and costs; and

d) Such further relief as this Court deems equitable and just.

Q. Count XVII – Nevada False Claims Act

602. Relator realleges and hereby incorporates by reference each and every allegation contained in all paragraphs of this complaint.

603. This is a *qui tam* action brought by Relator and the State of Nevada to recover treble damages and civil penalties under the Nevada False Claims Act ("NFCA"), NEV. REV. STAT. §§ 357.010–357.250.

604. The NFCA provides that any person who, with or without specific intent to defraud:

> (a) Knowingly presents or causes to be presented a false or fraudulent claim for payment or approval[; or]
> (b) Knowingly makes or uses, or causes to be made or used, a false record or statement that is material to a false or fraudulent claim[; or . . .]
> (i) Conspires to commit any of the acts set forth [above,]

NEV. REV. STAT. § 357.040(1), is liable to the State of Nevada for a civil penalty of $11,181 to $22,363 for each violation of the NFCA, plus three times the amount of damages which the State of Nevada sustains because of the violation. *See* 28 C.F.R. § 85.5; NEV. REV. STAT. § 357.040(2)(c).

1. Presentment of False and/or Fraudulent Claims (NEV. REV. STAT. § 357.040(1)(a))

605. From at least 2016 to the present, the following Defendants knowingly presented, or caused to be presented, false and/or fraudulent claims to the State of Nevada and its political subdivisions for payment or approval: Microsoft Corporation; Microsoft Licensing, G.P.; En Pointe Technologies Sales, LLC; PCM, Inc.; and SHI International Corporation.

606. The above-named Defendants fraudulently induced the State of Nevada and its political subdivisions to enter into contracts and agreements for cloud computing services by making false statements regarding the cloud services' government exclusivity and security.

Defendants made these false statements in marketing and advertising materials as well as in the contracts and agreements themselves.

607. The above-named Defendants submitted claims for payment to the State of Nevada and its political subdivisions under the contracts and agreements at issue, which were both fraudulently induced and/or contain false statements and certifications.

608. The above-named Defendants also made false certifications in the contracts and agreements at issue as to compliance with applicable laws.

609. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the NFCA.

610. The above-named Defendants' knowing submission, or causation of submission, of false and/or fraudulent claims had the potential to influence the State of Nevada and its political subdivisions' payment decision and was material to the State of Nevada and its political subdivisions' decision to pay the claims.

611. The above-named Defendants' misrepresentations regarding the cloud services at issue and their compliance with the applicable standards for cloud computing are material because they went to the very essence of the bargain for which the State of Nevada and its political subdivisions contracted. Had the State of Nevada and its political subdivisions known of Defendants' fraudulent non-compliance, which resulted in the submission of ineligible false claims for reimbursement, they would not have paid the claims.

612. The above-named Defendants' presentment, or causation of presentment, of false and/or fraudulent claims to the State of Nevada and its political subdivisions was a foreseeable factor in the State of Nevada and its political subdivisions' loss and a consequence of

Defendants' fraudulent scheme. By virtue of the above-named Defendants' actions, the State of Nevada and its political subdivisions have suffered damages.

2. Making or Using False Records or Statements Material to False and/or Fraudulent Claims (NEV. REV. STAT. § 357.040(1)(b))

613. From at least 2016 to the present, the above-named Defendants knowingly made, used, or caused to be made or used, false records or statements that were material to false and/or fraudulent claims paid or approved by the State of Nevada and its political subdivisions. These false records or statements include those made on websites and in other marketing materials.

614. The above-named Defendants knowingly and fraudulently used the false statements in their marketing materials and websites both to induce the State of Nevada and its political subdivisions to enter into the contracts and agreements at issue and to get false and/or fraudulent claims made pursuant to those contracts paid or approved by the State of Nevada and its political subdivisions.

615. The above-named Defendants' false statements or records, or causation of false statements or records, had the potential to influence the State of Nevada and its political subdivisions' payment decision and were material to the State of Nevada and its political subdivisions' decision to pay the claims.

616. The above-named Defendants' false statements regarding the exclusivity and deployment models of the cloud services at issue were material because they went to the very essence of the bargain for which the State of Nevada and its political subdivisions contracted. Had the State of Nevada and its political subdivisions known of Defendants' fraudulent misrepresentations regarding the cloud services at issue, which resulted in the submission of ineligible false and/or fraudulent claims for reimbursement, then the State of Nevada and its

political subdivisions would not have entered into the contracts and agreements at issue or paid claims under those contracts and agreements.

617. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the NFCA.

618. The above-named Defendants' submission, or causation of submission, of false records and statements material to false and/or fraudulent claims was a foreseeable factor in the State of Nevada's loss and a consequence of Defendants' scheme. By virtue of Defendants' actions, the State of Nevada and its political subdivisions have suffered damages.

3. Conspiracy (NEV. REV. STAT. § 357.040(1)(i))

619. From at least 2016 to the present, the above-named Defendants conspired together to: (1) fraudulently induce the State of Nevada and its political subdivisions to enter into contracts and agreements with them; and (2) submit or cause the submission of false and/or fraudulent claims under those contracts and agreements to the State of Nevada and its political subdivisions.

620. Microsoft entered into agreements with the State of Nevada and its political subdivisions that are part and parcel of the above-named Reseller Defendants' contracts with the State of Nevada and its political subdivisions for the cloud services at issue.

621. The above-named Reseller Defendants, having issued all invoices for the specific products at issue, knew that cloud services marketed as "for Government" which utilized Microsoft's "fake SKU" included commercial cloud services, and were therefore not actually "for Government."

622. The above-named Defendants' conspiracy had the potential to influence the State of Nevada and its political subdivisions' payment decision because the State of Nevada and its

political subdivisions would not have entered into the contracts and agreements at issue or paid claims under them had they known that they were not receiving true "government cloud" services.

* * *

623. WHEREFORE, Relator respectfully requests that the Court enter judgment against Defendants, and award the following:

To the STATE OF NEVADA:

a) Three times the amount of damages that the State of Nevada has sustained as a result of Defendants' fraudulent and illegal practices;

b) Civil penalties against Defendants up to the maximum allowed by law for each violation of NEV. REV. STAT. § 357.040(1); and

c) All costs incurred in bringing this action.

To RELATOR:

a) The maximum amount allowed pursuant to NEV. REV. STAT. § 357.210 and/or any other applicable provision of law;

b) Reimbursement for reasonable expenses Relator incurred in connection with this action;

c) An award of reasonable attorney's fees and costs; and

d) Such further relief as this Court deems equitable and just.

R. Count XVIII – New Jersey False Claims Act

624. Relator realleges and hereby incorporates by reference each and every allegation contained in all paragraphs of this complaint.

625. This is a *qui tam* action brought by Relator and the State of New Jersey to recover treble damages and civil penalties under the New Jersey False Claims Act ("NJFCA"), N.J. STAT. ANN. §§ 2A:32C-1–2A:32C-18.

626. The NJFCA provides that any person who:

> (a) Knowingly presents or causes to be presented to an employee, officer or agent of the State, or to any contractor, grantee, or other recipient of State funds, a false or fraudulent claim for payment or approval; [or]
> (b) Knowingly makes, uses, or causes to be made or used a false record or statement to get a false or fraudulent claim paid or approved by the State; [or]
> (c) Conspires to defraud the State by getting a false or fraudulent claim allowed or paid by the State[,]

N.J. STAT. ANN. § 2A:32C-3, is liable to the State of New Jersey for a civil penalty of $11,181 to $22,363 for each violation of the NJFCA, plus three times the amount of damages which the State of New Jersey sustains because of the violation. *See* 28 C.F.R. § 85.5; N.J. STAT. ANN. § 2A:32C-3.

1. Presentment of False and/or Fraudulent Claims (N.J. STAT. ANN. § 2A:32C-3(a))

627. From at least 2016 to the present, the following Defendants knowingly presented, or caused to be presented, false and/or fraudulent claims to the State of New Jersey and its political subdivisions for payment or approval: Microsoft Corporation; CDW Government, LLC; Dell Marketing, L.P.; The Henson Group, Inc.; and Planet Technologies, Inc..

628. The above-named Defendants fraudulently induced the State of New Jersey and its political subdivisions to enter into contracts and agreements for cloud computing services by making false statements regarding the cloud services' government exclusivity and security. Defendants made these false statements in marketing and advertising materials and in the contracts and agreements themselves.

629. The above-named Defendants submitted claims for payment to the State of New Jersey and its political subdivisions under the contracts and agreements at issue, which were fraudulently induced.

630. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the NJFCA.

631. The above-named Defendants' knowing submission, or causation of submission, of false and/or fraudulent claims had the potential to influence the State of New Jersey and its political subdivisions' payment decision and was material to the State of New Jersey and its political subdivisions' decision to pay the claims.

632. The above-named Defendants' misrepresentations regarding the cloud services at issue and their compliance with the applicable standards for cloud computing are material because they went to the very essence of the bargain for which the State of New Jersey and its political subdivisions contracted. Had the State of New Jersey and its political subdivisions known of Defendants' fraudulent non-compliance, which resulted in the submission of ineligible false claims for reimbursement, they would not have paid the claims.

633. The above-named Defendants' presentment or causation of presentment, of false and/or fraudulent claims to the State of New Jersey and its political subdivisions was a foreseeable factor in the State of New Jersey and its political subdivisions' loss and a consequence of Defendants' fraudulent scheme. By virtue of the above-named Defendants' actions, the State of New Jersey and its political subdivisions have suffered damages.

2. Making or Using False Records or Statements to Get False and/or Fraudulent Claims Paid (N.J. STAT. ANN. § 2A:32C-3(b))

634. From at least 2016 to the present, the above-named Defendants knowingly made, used, or caused to be made or used, false records or statements to get false and/or fraudulent claims paid or approved by the State of New Jersey and its political subdivisions. These false records or statements include those made on websites and in other marketing materials.

635. The above-named Defendants knowingly and fraudulently used the false statements in their marketing materials and websites both to induce the State of New Jersey and its political subdivisions to enter into the contracts and agreements at issue and to get false and/or fraudulent claims made pursuant to those contracts paid or approved by the State of New Jersey and its political subdivisions.

636. The above-named Defendants' false statements or records, or causation of false statements or records, had the potential to influence the State of New Jersey and its political subdivisions' payment decision and were material to the State of New Jersey and its political subdivisions' decision to pay the claims.

637. The above-named Defendants' false statements regarding the exclusivity and deployment models of the cloud services at issue were material because they went to the very essence of the bargain for which the State of New Jersey and its political subdivisions contracted. Had the State of New Jersey and its political subdivisions known of Defendants' fraudulent misrepresentations regarding the cloud services at issue, which resulted in the submission of ineligible false and/or fraudulent claims for reimbursement, then the State of New Jersey and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under those contracts and agreements.

638. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the NJFCA.

639. The above-named Defendants' submission, or causation of submission, of false records and statements to get false and/or fraudulent claims paid or approved was a foreseeable factor in the State of New Jersey's loss and a consequence of Defendants' scheme. By virtue of

Defendants' actions, the State of New Jersey and its political subdivisions have suffered damages.

3. Conspiracy (N.J. STAT. ANN. § 2A:32C-3(c))

640. From at least 2016 to the present, the above-named Defendants conspired together to: (1) fraudulently induce the State of New Jersey and its political subdivisions to enter into contracts and agreements with them; and (2) submit or cause the submission of false and/or fraudulent claims under those contracts and agreements to the State of New Jersey and its political subdivisions.

641. Microsoft entered into agreements with the State of New Jersey and its political subdivisions that are part and parcel of the above-named Reseller Defendants' contracts with the State of New Jersey and its political subdivisions for the cloud services at issue.

642. The above-named Reseller Defendants, having issued all invoices for the specific products at issue, knew that cloud services marketed as "for Government" which utilized Microsoft's "fake SKU" included commercial cloud services, and were therefore not actually "for Government."

643. The above-named Defendants' conspiracy had the potential to influence the State of New Jersey and its political subdivisions' payment decision because the State of New Jersey and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under them had they known that they were not receiving true "government cloud" services.

* * *

644. WHEREFORE, Relator respectfully requests that the Court enter judgment against Defendants, and award the following:

To the STATE OF NEW JERSEY:

a) Three times the amount of damages that the State of New Jersey has sustained as a result of Defendants' fraudulent and illegal practices;

b) Civil penalties against Defendants up to the maximum allowed by law for each violation of N.J. STAT. ANN. § 2A:32C-3; and

c) All costs incurred in bringing this action.

To RELATOR:

a) The maximum amount allowed pursuant to N.J. STAT. ANN. § 2A:32C-7 and/or any other applicable provision of law;

b) Reimbursement for reasonable expenses Relator incurred in connection with this action;

c) An award of reasonable attorney's fees and costs; and

d) Such further relief as this Court deems equitable and just.

S. Count XIX – New Mexico Fraud Against Taxpayers Act

645. Relator realleges and hereby incorporates by reference each and every allegation contained in all paragraphs of this complaint.

646. This is a *qui tam* action brought by Relator and the State of New Mexico to recover treble damages and civil penalties under the New Mexico Fraud Against Taxpayers Act ("FATA"), N.M. STAT. ANN. §§ 44-9-1–44-9-14.

647. FATA provides that a person shall not:

(1) knowingly present, or cause to be presented, to an employee, officer or agent of the state or a political subdivision or to a contractor, grantee or other recipient of state or political subdivision funds a false or fraudulent claim for payment or approval; [or]
(2) knowingly make or use, or cause to be made or used, a false, misleading or fraudulent record or statement to obtain or support the approval of or the payment on a false or fraudulent claim; [or]
(3) conspire to defraud the state or a political subdivision by obtaining approval or payment on a false or fraudulent claim[.]

N.M. STAT. ANN. § 44-9-3(A). Anyone who commits one of the above violations is liable to the State of New Mexico for a civil penalty of $5,000 to $10,000 for each violation of FATA, plus three times the amount of damages which the State of New Mexico sustains because of the violation. *See* N.M. STAT. ANN. § 44-9-3(C)(1)–(2).

1. Presentment of False and/or Fraudulent Claims (N.M. STAT. ANN. § 44-9-3(A)(1))

648. From at least 2014 to the present, the following Defendants knowingly presented, or caused to be presented, false and/or fraudulent claims to the State of New Mexico and its political subdivisions for payment or approval: Microsoft Corporation; Microsoft Licensing, G.P.; and SHI International Corporation.

649. The above-named Defendants fraudulently induced the State of New Mexico and its political subdivisions to enter into contracts and agreements for cloud computing services by making false statements regarding the cloud services' government exclusivity and security. Defendants made these false statements in marketing and advertising materials as well as in the contracts and agreements themselves.

650. The above-named Defendants also made false certifications in the contracts and agreements at issue as to compliance with applicable laws.

651. The above-named Defendants submitted claims for payment to the State of New Mexico and its political subdivisions under the contracts and agreements at issue, which were both fraudulently induced and/or contain false statements and certifications.

652. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated FATA.

653. The above-named Defendants' knowing submission or causation of submission of false and/or fraudulent claims had the potential to influence the State of New Mexico and its

political subdivisions' payment decision and was material to the State of New Mexico and its political subdivisions' decision to pay the claims.

654. The above-named Defendants' misrepresentations regarding the cloud services at issue and their compliance with the applicable standards for cloud computing are material because they went to the very essence of the bargain for which the State of New Mexico and its political subdivisions contracted. Had the State of New Mexico and its political subdivisions known of Defendants' fraudulent non-compliance, which resulted in the submission of ineligible false claims for reimbursement, they would not have paid the claims.

655. The above-named Defendants' presentment or causation of presentment, of false and/or fraudulent claims to the State of New Mexico and its political subdivisions was a foreseeable factor in the State of New Mexico and its political subdivisions' loss and a consequence of Defendants' fraudulent scheme. By virtue of the above-named Defendants' actions, the State of New Mexico and its political subdivisions have suffered damages.

2. Making or Using False, Misleading, and/or Fraudulent Records or Statements to Get False and/or Fraudulent Claims Paid (N.M. STAT. ANN. § 44-9-3(A)(2))

656. From at least 2014 to the present, the above-named Defendants knowingly made, used, or caused to be made or used, false, misleading, and/or fraudulent records or statements to get false and/or fraudulent claims paid or approved by the State of New Mexico and its political subdivisions. These false, misleading, and/or fraudulent records or statements include those made on websites and in other marketing materials.

657. The above-named Defendants knowingly and fraudulently used the false, misleading, and/or fraudulent statements in their marketing materials and websites both to induce the State of New Mexico and its political subdivisions to enter into the contracts and agreements

at issue and to get false and/or fraudulent claims made pursuant to those contracts paid or approved by the State of New Mexico and its political subdivisions.

658. The above-named Defendants' false, misleading, and/or fraudulent statements or records, or causation of false statements or records, had the potential to influence the State of New Mexico and its political subdivisions' payment decision and were material to the State of New Mexico and its political subdivisions' decision to pay the claims.

659. The above-named Defendants' false, misleading, and/or fraudulent statements regarding the exclusivity and deployment models of the cloud services at issue were material because they went to the very essence of the bargain for which the State of New Mexico and its political subdivisions contracted. Had the State of New Mexico and its political subdivisions known of Defendants' fraudulent misrepresentations regarding the cloud services at issue, which resulted in the submission of ineligible false and/or fraudulent claims for reimbursement, then the State of New Mexico and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under those contracts and agreements.

660. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated FATA.

661. The above-named Defendants' submission, or causation of submission, of false records and statements to get false and/or fraudulent claims paid or approved was a foreseeable factor in the State of New Mexico's loss and a consequence of Defendants' scheme. By virtue of Defendants' actions, the State of New Mexico and its political subdivisions have suffered damages.

3. Conspiracy (N.M. STAT. ANN. § 44-9-3(A)(3))

662. From at least 2014 to the present, the above-named Defendants conspired together to defraud the State of New Mexico by obtaining payment or approval of false claims. Defendants accomplished this by: (1) fraudulently inducing the State of New Mexico and its political subdivisions to enter into contracts and agreements with them; and (2) submitting or causing the submission of false and/or fraudulent claims under those contracts and agreements to the State of New Mexico and its political subdivisions.

663. Microsoft entered into agreements with the State of New Mexico and its political subdivisions that are part and parcel of the above-named Reseller Defendants' contracts with the State of New Mexico and its political subdivisions for the cloud services at issue.

664. The above-named Reseller Defendants, having issued all invoices for the specific products at issue, knew that cloud services marketed as "for Government" which utilized Microsoft's "fake SKU" included commercial cloud services, and were therefore not actually "for Government."

665. The above-named Defendants' conspiracy had the potential to influence the State of New Mexico and its political subdivisions' payment decision because the State of New Mexico and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under them had they known that they were not receiving true "government cloud" services.

* * *

666. WHEREFORE, Relator respectfully requests that the Court enter judgment against Defendants, and award the following:

To the STATE OF NEW MEXICO:

a) Three times the amount of damages that the State of New Mexico has sustained as a result of Defendants' fraudulent and illegal practices;

b) Civil penalties against Defendants up to the maximum allowed by law for each violation of N.M. STAT. ANN. § 44-9-3(A); and

c) All costs incurred in bringing this action.

To RELATOR:

a) The maximum amount allowed pursuant to N.M. STAT. ANN. § 44-9-7 and/or any other applicable provision of law;

b) Reimbursement for reasonable expenses Relator incurred in connection with this action;

c) An award of reasonable attorney's fees and costs; and

d) Such further relief as this Court deems equitable and just.

T. Count XX – North Carolina False Claims Act

667. Relator realleges and hereby incorporates by reference each and every allegation contained in all paragraphs of this complaint.

668. This is a *qui tam* action brought by Relator and the State of North Carolina to recover treble damages and civil penalties under the North Carolina False Claims Act ("NCFCA"), N.C. GEN. STAT. ANN. §§ 1-605–1-618.

669. The NCFCA provides that any person who:

(1) Knowingly presents or causes to be presented a false or fraudulent claim for payment or approval[; or]
(2) Knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim[; or]
(3) Conspires to commit a violation of [the above paragraphs,]

N.C. GEN. STAT. ANN. § 1-607(a), is liable to the State of North Carolina for a civil penalty of $11,181 to $22,363 for each violation of the NCFCA, plus three times the amount of damages

which the State of North Carolina sustains because of the violation. *See* 28 C.F.R. § 85.5; N.C. GEN. STAT. ANN. § 1-607(a).

1. Presentment of False and/or Fraudulent Claims (N.C. GEN. STAT. ANN. § 1-607(a)(1))

670. From at least 2014 to the present, the following Defendants knowingly presented, or caused to be presented, false and/or fraudulent claims to the State of North Carolina and its political subdivisions for payment or approval: Microsoft Corporation; Dell Marketing, L.P.; PCM, Inc.; PCMG, Inc.; Planet Technologies; SHI International Corporation; and Software One, Inc..

671. The above-named Defendants fraudulently induced the State of North Carolina and its political subdivisions to enter into contracts and agreements for cloud computing services by making false statements regarding the cloud services' government exclusivity and security. Defendants made these false statements in marketing and advertising materials as well as in the contracts and agreements themselves.

672. The above-named Defendants submitted claims for payment to the State of North Carolina and its political subdivisions under the contracts and agreements at issue, which were both fraudulently induced and/or contain false statements and certifications.

673. The above-named Defendants also made false certifications in the contracts and agreements at issue as to compliance with applicable laws.

674. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the NCFCA.

675. The above-named Defendants' knowing submission, or causation of submission, of false and/or fraudulent claims had the potential to influence the State of North Carolina and its

political subdivisions' payment decision and was material to the State of North Carolina and its political subdivisions' decision to pay the claims.

676. The above-named Defendants' misrepresentations regarding the cloud services at issue and their compliance with the applicable standards for cloud computing are material because they went to the very essence of the bargain for which the State of North Carolina and its political subdivisions contracted. Had the State of North Carolina and its political subdivisions known of Defendants' fraudulent non-compliance, which resulted in the submission of ineligible false claims for reimbursement, they would not have paid the claims.

677. The above-named Defendants' presentment or causation of presentment, of false and/or fraudulent claims to the State of North Carolina and its political subdivisions was a foreseeable factor in the State of North Carolina and its political subdivisions' loss and a consequence of Defendants' fraudulent scheme. By virtue of the above-named Defendants' actions, the State of North Carolina and its political subdivisions have suffered damages.

2. Making or Using False Records or Statements Material to False and/or Fraudulent Claims (N.C. GEN. STAT. ANN. § 1-607(a)(2))

678. From at least 2014 to the present, the above-named Defendants knowingly made, used, or caused to be made or used, false records or statements material to false and/or fraudulent claims paid or approved by the State of North Carolina and its political subdivisions. These false records or statements include those made on websites and in other marketing materials.

679. The above-named Defendants knowingly and fraudulently used the false records or statements in their marketing materials and websites both to induce the State of North Carolina and its political subdivisions to enter into the contracts and agreements at issue and to get false and/or fraudulent claims made pursuant to those contracts paid or approved by the State of North Carolina and its political subdivisions.

680. The above-named Defendants' false statements or records, or causation of false statements or records, had the potential to influence the State of North Carolina and its political subdivisions' payment decision and were material to the State of North Carolina and its political subdivisions' decision to pay the claims.

681. The above-named Defendants' false statements regarding the exclusivity and deployment models of the cloud services at issue were material because they went to the very essence of the bargain for which the State of North Carolina and its political subdivisions contracted. Had the State of North Carolina and its political subdivisions known of Defendants' fraudulent misrepresentations regarding the cloud services at issue, which resulted in the submission of ineligible false and/or fraudulent claims for reimbursement, then the State of North Carolina and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under those contracts and agreements.

682. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the NCFCA.

683. The above-named Defendants' submission, or causation of submission, of false records and statements material to false and/or fraudulent claims was a foreseeable factor in the State of North Carolina's loss and a consequence of Defendants' scheme. By virtue of Defendants' actions, the State of North Carolina and its political subdivisions have suffered damages.

3. Conspiracy (N.C. GEN. STAT. ANN. § 1-607(a)(3))

684. From at least 2014 to the present, the above-named Defendants conspired together to: (1) fraudulently induce the State of North Carolina and its political subdivisions to enter into contracts and agreements with them; and (2) submit or cause the submission of false and/or

fraudulent claims under those contracts and agreements to the State of North Carolina and its political subdivisions.

685. Microsoft entered into agreements with the State of North Carolina and its political subdivisions that are part and parcel of the above-named Reseller Defendants' contracts with the State of North Carolina and its political subdivisions for the cloud services at issue.

686. The above-named Reseller Defendants, having issued all invoices for the specific products at issue, knew that cloud services marketed as "for Government" which utilized Microsoft's "fake SKU" included commercial cloud services, and were therefore not actually "for Government."

687. The above-named Defendants' conspiracy had the potential to influence the State of North Carolina and its political subdivisions' payment decision because the State of North Carolina and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under them had they known that they were not receiving true "government cloud" services.

* * *

688. WHEREFORE, Relator respectfully requests that the Court enter judgment against Defendants, and award the following:

To the STATE OF NORTH CAROLINA:

a) Three times the amount of damages that the State of North Carolina has sustained as a result of Defendants' fraudulent and illegal practices;

b) Civil penalties against Defendants up to the maximum allowed by law for each violation of N.C. GEN. STAT. ANN. § 1-607(a); and

c) All costs incurred in bringing this action.

To RELATOR:

a) The maximum amount allowed pursuant to N.C. GEN. STAT. ANN. § 1-610 and/or any other applicable provision of law;

b) Reimbursement for reasonable expenses Relator incurred in connection with this action;

c) An award of reasonable attorney's fees and costs; and

d) Such further relief as this Court deems equitable and just.

U. Count XXI – Rhode Island False Claims Act

689. Relator realleges and hereby incorporates by reference each and every allegation contained in all paragraphs of this complaint.

690. This is a *qui tam* action brought by Relator and the State of Rhode Island to recover treble damages and civil penalties under the Rhode Island False Claims Act ("RIFCA"), R.I. GEN. LAWS ANN. §§ 9-1.1-1–9-1.1.-9.

691. The RIFCA provides that any person who:

(1) Knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval; [or]
(2) Knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim; [or]
(3) Conspires to commit a violation of [the above paragraphs,]

R.I. GEN. LAWS ANN. § 9-1.1-3(a), is liable to the State of Rhode Island for a civil penalty of $11,181 to $22,363 for each violation of the RIFCA, plus three times the amount of damages which the State of Rhode Island sustains because of the violation. *See* 28 C.F.R. § 85.5; R.I. GEN. LAWS ANN. § 9-1.1.-3(a).

1. Presentment of False and/or Fraudulent Claims (R.I. GEN. LAWS ANN. § 9-1.1-3(a)(1))

692. From at least 2015 to the present, the following Defendants knowingly presented, or caused to be presented, false and/or fraudulent claims to the State of Rhode Island and its

political subdivisions for payment or approval: Microsoft Corporation; Dell Marketing, L.P.; En Pointe Technologies Sales, LLC; and PCM, Inc.

693. The above-named Defendants fraudulently induced the State of Rhode Island and its political subdivisions to enter into contracts and agreements for cloud computing services by making false statements regarding the cloud services' government exclusivity and security. Defendants made these false statements in marketing and advertising materials as well as in the contracts and agreements themselves.

694. The above-named Defendants submitted claims for payment to the State of Rhode Island and its political subdivisions under the contracts and agreements at issue, which were fraudulently induced and/or contain false statements and certifications.

695. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the RIFCA.

696. The above-named Defendants' knowing submission, or causation of submission, of false and/or fraudulent claims had the potential to influence the State of Rhode Island and its political subdivisions' payment decision and was material to the State of Rhode Island and its political subdivisions' decision to pay the claims.

697. The above-named Defendants' misrepresentations regarding the cloud services at issue and their compliance with the applicable standards for cloud computing are material because they went to the very essence of the bargain for which the State of Rhode Island and its political subdivisions contracted. Had the State of Rhode Island and its political subdivisions known of Defendants' fraudulent non-compliance, which resulted in the submission of ineligible false claims for reimbursement, they would not have paid the claims.

698. The above-named Defendants' presentment or causation of presentment, of false and/or fraudulent claims to the State of Rhode Island and its political subdivisions was a foreseeable factor in the State of Rhode Island and its political subdivisions' loss and a consequence of Defendants' fraudulent scheme. By virtue of the above-named Defendants' actions, the State of Rhode Island and its political subdivisions have suffered damages.

2. Making or Using False Records or Statements Material to False and/or Fraudulent Claims (R.I. GEN. LAWS ANN. § 9-1.1-3(a)(2))

699. From at least 2015 to the present, the above-named Defendants knowingly made, used, or caused to be made or used, false records or statements material to false and/or fraudulent claims paid or approved by the State of Rhode Island and its political subdivisions. These false records or statements include those made on websites and in other marketing materials.

700. The above-named Defendants knowingly and fraudulently used the false records or statements in their marketing materials and websites both to induce the State of Rhode Island and its political subdivisions to enter into the contracts and agreements at issue and to get false and/or fraudulent claims made pursuant to those contracts paid or approved by the State of Rhode Island and its political subdivisions.

701. The above-named Defendants' false statements or records, or causation of false statements or records, had the potential to influence the State of Rhode Island and its political subdivisions' payment decision and were material to the State of Rhode Island and its political subdivisions' decision to pay the claims.

702. The above-named Defendants' false statements regarding the exclusivity and deployment models of the cloud services at issue were material because they went to the very essence of the bargain for which the State of Rhode Island and its political subdivisions contracted. Had the State of Rhode Island and its political subdivisions known of Defendants'

fraudulent misrepresentations regarding the cloud services at issue, which resulted in the submission of ineligible false and/or fraudulent claims for reimbursement, then the State of Rhode Island and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under those contracts and agreements.

703. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the RIFCA.

704. The above-named Defendants' submission, or causation of submission, of false records and statements material to false and/or fraudulent claims was a foreseeable factor in the State of Rhode Island's loss and a consequence of Defendants' scheme. By virtue of Defendants' actions, the State of Rhode Island and its political subdivisions have suffered damages.

3. Conspiracy (R.I. GEN. LAWS ANN. § 9-1.1-3(a)(3))

705. From at least 2015 to the present, the above-named Defendants conspired together to: (1) fraudulently induce the State of Rhode Island and its political subdivisions to enter into contracts and agreements with them; and (2) submit or cause the submission of false and/or fraudulent claims under those contracts and agreements to the State of Rhode Island and its political subdivisions.

706. Microsoft entered into agreements with the State of Rhode Island and its political subdivisions that are part and parcel of the above-named Reseller Defendants' contracts with the State of Rhode Island and its political subdivisions for the cloud services at issue.

707. The above-named Reseller Defendants, having issued all invoices for the specific products at issue, knew that cloud services marketed as "for Government" which utilized

Microsoft's "fake SKU" included commercial cloud services, and were therefore not actually "for Government."

708. The above-named Defendants' conspiracy had the potential to influence the State of Rhode Island and its political subdivisions' payment decision because the State of Rhode Island and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under them had they known that they were not receiving true "government cloud" services.

* * *

709. WHEREFORE, Relator respectfully requests that the Court enter judgment against Defendants, and award the following:

To the STATE OF RHODE ISLAND:

a) Three times the amount of damages that the State of Rhode Island has sustained as a result of Defendants' fraudulent and illegal practices;

b) Civil penalties against Defendants up to the maximum allowed by law for each violation of R.I. GEN. LAWS ANN. § 9-1.1-3; and

c) All costs incurred in bringing this action.

To RELATOR:

a) The maximum amount allowed pursuant to R.I. GEN. LAWS ANN. § 9-1.1-4(d) and/or any other applicable provision of law;

b) Reimbursement for reasonable expenses Relator incurred in connection with this action;

c) An award of reasonable attorney's fees and costs; and

d) Such further relief as this Court deems equitable and just.

V. Count XXII – Tennessee False Claims Act

710. Relator realleges and hereby incorporates by reference each and every allegation contained in all paragraphs of this complaint.

711. This is a *qui tam* action brought by Relator and the State of Tennessee to recover treble damages and civil penalties under the Tennessee False Claims Act ("TFCA"), TENN. CODE ANN. §§ 4-18-101–4-18-108.

712. The TFCA provides that any person who:

> (1) Knowingly presents or causes to be presented to an officer or employee of the state or of any political subdivision thereof, a false or fraudulent claim for payment or approval; [or]
> (2) Knowingly makes, uses, or causes to be made or used a false record or statement to get a false claim paid or approved by the state or by any political subdivision; [or]
> (3) Conspires to defraud the state or any political subdivision by getting a false claim allowed or paid by the state or by any political subdivision; [or . . .]
> (9) Knowingly makes, uses, or causes to be made or used any false or fraudulent conduct, representation, or practice in order to procure anything of value directly or indirectly from the state or any political subdivision[,]

TENN. CODE ANN. § 4-18-103(a), is liable to the State of Tennessee for a civil penalty of $2,500 to $10,000 for each violation of the TFCA, plus three times the amount of damages which the State of Tennessee sustains because of the violation. *See id.*

1. Presentment of False and/or Fraudulent Claims (TENN. CODE ANN. § 4-18-103(a)(1))

713. From at least 2016 to the present, the following Defendants knowingly presented, or caused to be presented, false and/or fraudulent claims to the State of Tennessee and its political subdivisions for payment or approval: Microsoft Corporation; Dell Marketing, L.P.; and Liftoff, LLC.

714. The above-named Defendants fraudulently induced the State of Tennessee and its political subdivisions to enter into contracts and agreements for cloud computing services by

making false statements regarding the cloud services' government exclusivity and security. Defendants made these false statements in marketing and advertising materials as well as in the contracts and agreements themselves.

715. The above-named Defendants also made false certifications in the contracts and agreements at issue as to compliance with applicable laws.

716. The above-named Defendants submitted claims for payment to the State of Tennessee and its political subdivisions under the contracts and agreements at issue, which were both fraudulently induced and/or contain false statements and certifications.

717. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the TFCA.

718. The above-named Defendants' knowing submission or causation of submission of false and/or fraudulent claims had the potential to influence the State of Tennessee and its political subdivisions' payment decision and was material to the State of Tennessee and its political subdivisions' decision to pay the claims.

719. The above-named Defendants' misrepresentations regarding the cloud services at issue and their compliance with the applicable standards for cloud computing are material because they went to the very essence of the bargain for which the State of Tennessee and its political subdivisions contracted. Had the State of Tennessee and its political subdivisions known of Defendants' fraudulent non-compliance, which resulted in the submission of ineligible false claims for reimbursement, they would not have paid the claims.

720. The above-named Defendants' presentment or causation of presentment, of false and/or fraudulent claims to the State of Tennessee and its political subdivisions was a foreseeable factor in the State of Tennessee and its political subdivisions' loss and a consequence of

Defendants' fraudulent scheme. By virtue of the above-named Defendants' actions, the State of Tennessee and its political subdivisions have suffered damages.

2. Making or Using False Records or Statements to Get False Claims Paid or Approved (TENN. CODE ANN. § 4-18-103(a)(2))

721. From at least 2016 to the present, the above-named Defendants knowingly made, used, or caused to be made or used, false records or statements to get false claims paid or approved by the State of Tennessee and its political subdivisions. These false, misleading, and/or fraudulent records or statements include those made on websites and in other marketing materials.

722. The above-named Defendants knowingly and fraudulently used the false statements in their marketing materials and websites both to induce the State of Tennessee and its political subdivisions to enter into the contracts and agreements at issue and to get false claims made pursuant to those contracts paid or approved by the State of Tennessee and its political subdivisions.

723. The above-named Defendants' false statements or records, or causation of false statements or records, had the potential to influence the State of Tennessee and its political subdivisions' payment decision and were material to the State of Tennessee and its political subdivisions' decision to pay the claims.

724. The above-named Defendants' false statements regarding the exclusivity and deployment models of the cloud services at issue were material because they went to the very essence of the bargain for which the State of Tennessee and its political subdivisions contracted. Had the State of Tennessee and its political subdivisions known of Defendants' false statements regarding the cloud services at issue, which resulted in the submission of ineligible false claims for reimbursement, then the State of Tennessee and its political subdivisions would not have

entered into the contracts and agreements at issue or paid claims under those contracts and agreements.

725. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the TFCA.

726. The above-named Defendants' submission, or causation of submission, of false records and statements to get false claims paid or approved was a foreseeable factor in the State of Tennessee's loss and a consequence of Defendants' scheme. By virtue of Defendants' actions, the State of Tennessee and its political subdivisions have suffered damages.

3. Conspiracy (TENN. CODE ANN. § 4-18-103(a)(3))

727. From at least 2016 to the present, the above-named Defendants conspired together to defraud the State of Tennessee by getting false claims paid or allowed by the State and its political subdivisions. Defendants accomplished this by: (1) fraudulently inducing the State of Tennessee and its political subdivisions to enter into contracts and agreements with them; and (2) submitting or causing the submission of false and/or fraudulent claims under those contracts and agreements to the State of Tennessee and its political subdivisions.

728. Microsoft entered into agreements with the State of Tennessee and its political subdivisions that are part and parcel of the above-named Reseller Defendants' contracts with the State of Tennessee and its political subdivisions for the cloud services at issue.

729. The above-named Reseller Defendants, having issued all invoices for the specific products at issue, knew that cloud services marketed as "for Government" which utilized Microsoft's "fake SKU" included commercial cloud services, and were therefore not actually "for Government."

730. The above-named Defendants' conspiracy had the potential to influence the State of Tennessee and its political subdivisions' payment decision because the State of Tennessee and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under them had they known that they were not receiving true "government cloud" services.

4. False and/or Fraudulent Conduct, Representations, or Practices (TENN. CODE ANN. § 4-18-103(a)(9))

731. From at least 2016 to the present, the above-named Defendants knowingly made, used, or caused to be made or used false and/or fraudulent conduct, representations, and practices in order to procure contracts and the payment of claims from the State of Tennessee and its political subdivisions.

732. The above-named Defendants fraudulently induced the State of Tennessee and its political subdivisions to enter into contracts and agreements for cloud computing services by making false statements and misrepresentations regarding the cloud services' government exclusivity and security. Defendants made these false statements and misrepresentations in marketing and advertising materials as well as in the contracts and agreements themselves.

733. Defendants perpetuated this fraudulent scheme by failing to amend the contracts and agreements to reflect the true nature of the cloud services at issue—*i.e.*, that they were not entirely government-exclusive.

734. The above-named Defendants' fraudulent conduct had the potential to influence the State of Tennessee and its political subdivisions' payment decision because the State of Tennessee and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under them had they known that they were not receiving true "government cloud" services.

* * *

735. WHEREFORE, Relator respectfully requests that the Court enter judgment against Defendants, and award the following:

To the STATE OF TENNESSEE:

a) Three times the amount of damages that the State of Tennessee has sustained as a result of Defendants' fraudulent and illegal practices;

b) Civil penalties against Defendants up to the maximum allowed by law for each violation of TENN. CODE ANN. § 4-18-103(a); and

c) All costs incurred in bringing this action.

To RELATOR:

a) The maximum amount allowed pursuant to TENN. CODE ANN. § 4-18-104(g) and/or any other applicable provision of law;

b) Reimbursement for reasonable expenses Relator incurred in connection with this action;

c) An award of reasonable attorney's fees and costs; and

d) Such further relief as this Court deems equitable and just.

W. Count XXIII – Vermont False Claims Act

736. Relator realleges and hereby incorporates by reference each and every allegation contained in all paragraphs of this complaint.

737. This is a *qui tam* action brought by Relator and the State of Vermont to recover treble damages and civil penalties under the Vermont False Claims Act ("VTFCA"), VT. STAT. ANN. tit. 32, §§ 630–642.

738. The VTFCA provides that no person shall:

(1) knowingly present, or cause to be presented, a false or fraudulent claim for payment or approval; [or]
(2) knowingly make, use, or cause to be made or used, a false record or statement material to a false or fraudulent claim; [or] . . .

> (8) enter into a written agreement or contract with an official of the State [of Vermont] or its agent knowing the information contained therein is false; [or]
> . . .
> (12) conspire to commit a violation of [the VFCA,]

VT. STAT. ANN., tit. 32, § 631(a), is liable to the State of Vermont for a civil penalty of $11,181 to $22,363 for each violation of the VTFCA, plus three times the amount of damages which the State of Vermont sustains because of the violation. *See* 28 C.F.R. § 85.5; VT. STAT. ANN., tit. 32, § 631(b).

1. Presentment of False and/or Fraudulent Claims (VT. STAT. ANN., tit. 32, § 631(a)(1))

739. From at least 2016 to the present, the following Defendants knowingly presented, or caused to be presented, false and/or fraudulent claims to the State of Vermont and its political subdivisions for payment or approval: Microsoft Corporation; Aerie Consulting, LLC; CDW Corporation; and CDW Government, LLC.

740. The above-named Defendants fraudulently induced the State of Vermont and its political subdivisions to enter into contracts and agreements for cloud computing services by making false statements regarding the cloud services' government exclusivity and security. Defendants made these false statements in marketing and advertising materials and in the contracts and agreements themselves.

741. The above-named Defendants submitted claims for payment to the State of Vermont and its political subdivisions under the contracts and agreements at issue, which were both fraudulently induced and/or contain false statements and certifications.

742. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the VFCA.

743. The above-named Defendants' knowing submission or causation of submission of false and/or fraudulent claims had the potential to influence the State of Vermont and its political subdivisions' payment decision and was material to the State of Vermont and its political subdivisions' decision to pay the claims.

744. The above-named Defendants' misrepresentations regarding the cloud services at issue and their compliance with the applicable standards for cloud computing are material because they went to the very essence of the bargain for which the State of Vermont and its political subdivisions contracted. Had the State of Vermont and its political subdivisions known of Defendants' fraudulent non-compliance, which resulted in the submission of ineligible false claims for reimbursement, they would not have paid the claims.

745. The above-named Defendants' presentment or causation of presentment, of false and/or fraudulent claims to the State of Vermont and its political subdivisions was a foreseeable factor in the State of Vermont and its political subdivisions' loss and a consequence of Defendants' fraudulent scheme. By virtue of the above-named Defendants' actions, the State of Vermont and its political subdivisions have suffered damages.

2. Making or Using False Records or Statements Material to False and/or Fraudulent Claims (VT. STAT. ANN., tit. 32, § 631(a)(2))

746. From at least 2016 to the present, the above-named Defendants knowingly made, used, or caused to be made or used, false records or statements material to false and/or fraudulent claims. These false, misleading, and/or fraudulent records or statements include those made on websites and in other marketing materials.

747. The above-named Defendants knowingly and fraudulently used the false statements in their marketing materials and websites both to induce the State of Vermont and its political subdivisions to enter into the contracts and agreements at issue and to get false and/or

fraudulent claims made pursuant to those contracts paid or approved by the State of Vermont and its political subdivisions.

748. The above-named Defendants' false statements or records, or causation of false statements or records, had the potential to influence the State of Vermont and its political subdivisions' payment decision and were material to the State of Vermont and its political subdivisions' decision to pay the claims.

749. The above-named Defendants' false statements regarding the exclusivity and deployment models of the cloud services at issue were material because they went to the very essence of the bargain for which the State of Vermont and its political subdivisions contracted. Had the State of Vermont and its political subdivisions known of Defendants' false statements regarding the cloud services at issue, which resulted in the submission of ineligible false claims for reimbursement, then the State of Vermont and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under those contracts and agreements.

750. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the VFCA.

751. The above-named Defendants' submission, or causation of submission, of false records and statements material to false and/or fraudulent claims was a foreseeable factor in the State of Vermont's loss and a consequence of Defendants' scheme. By virtue of Defendants' actions, the State of Vermont and its political subdivisions have suffered damages.

3. Conspiracy (VT. STAT. ANN., tit. 32, § 631(a)(12))

752. From at least 2016 to the present, the above-named Defendants conspired together to: (1) fraudulently induce the State of Vermont and its political subdivisions to enter into

contracts and agreements with them; and (2) submit or cause the submission of false and/or fraudulent claims under those contracts and agreements to the State of Vermont and its political subdivisions.

753. Microsoft entered into agreements with the State of Vermont and its political subdivisions that are part and parcel of the above-named Reseller Defendants' contracts with the State of Vermont and its political subdivisions for the cloud services at issue.

754. The above-named Reseller Defendants, having issued all invoices for the specific products at issue, knew that cloud services marketed as "for Government" which utilized Microsoft's "fake SKU" included commercial cloud services, and were therefore not actually "for Government."

755. The above-named Defendants' conspiracy had the potential to influence the State of Vermont and its political subdivisions' payment decision because the State of Vermont and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under them had they known that they were not receiving true "government cloud" services.

* * *

756. WHEREFORE, Relator respectfully requests that the Court enter judgment against Defendants, and award the following:

To the STATE OF VERMONT:

a) Three times the amount of damages that the State of Vermont has sustained as a result of Defendants' fraudulent and illegal practices;

b) Civil penalties against Defendants up to the maximum allowed by law for each violation of VT. STAT. ANN., tit. 32, § 631(a); and

c) All costs incurred in bringing this action.

To RELATOR:

a) The maximum amount allowed pursuant to VT. STAT. ANN., tit. 32, § 635 and/or any other applicable provision of law;

b) Reimbursement for reasonable expenses Relator incurred in connection with this action;

c) An award of reasonable attorney's fees and costs; and

d) Such further relief as this Court deems equitable and just.

X. Count XXIV – Virginia Fraud Against Taxpayers Act

757. Relator realleges and hereby incorporates by reference each and every allegation contained in all paragraphs of this complaint.

758. This is a *qui tam* action brought by Relator and the Commonwealth of Virginia to recover treble damages and civil penalties under the Virginia Fraud Against Taxpayers Act ("VFATA"), VA. CODE ANN. §§ 8.01-216.1–8.01-216.19.

759. VFATA provides that any person who:

(1) Knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval; [or]
(2) Knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim; [or]
(3) Conspires to commit a violation of [the above paragraphs,]

VA. CODE ANN. § 8.01-216.3(A), is liable to the Commonwealth of Virginia for a civil penalty of $11,181 to $22,363 for each violation of VFATA, plus three times the amount of damages which the Commonwealth of Virginia sustains because of the violation. *See* 28 C.F.R. § 85.5; VA. CODE ANN. § 8.01-216.3(A).

1. Presentment of False and/or Fraudulent Claims (VA. CODE ANN. § 8.01-216.3(A)(1))

760. From at least 2012 to the present, the following Defendants knowingly presented, or caused to be presented, false and/or fraudulent claims to the Commonwealth of Virginia and

its political subdivisions for payment or approval: Microsoft Corporation; Insight Public Sector, Inc.; Liftoff, LLC; and SHI International Corporation.

761. The above-named Defendants fraudulently induced the Commonwealth of Virginia and its political subdivisions to enter into contracts and agreements for cloud computing services by making false statements regarding the cloud services' government exclusivity and security. Defendants made these false statements in marketing and advertising materials and in the contracts and agreements themselves.

762. The above-named Defendants submitted claims for payment to the Commonwealth of Virginia and its political subdivisions under the contracts and agreements at issue, which were both fraudulently induced and/or contain false statements and certifications.

763. Defendants also made false certifications in the contracts and agreements at issue as to their compliance with applicable laws.

764. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated VFATA.

765. The above-named Defendants' knowing submission or causation of submission of false and/or fraudulent claims had the potential to influence the Commonwealth of Virginia and its political subdivisions' payment decision and was material to the Commonwealth of Virginia and its political subdivisions' decision to pay the claims.

766. The above-named Defendants' misrepresentations regarding the cloud services at issue and their compliance with the applicable standards for cloud computing are material because they went to the very essence of the bargain for which the Commonwealth of Virginia and its political subdivisions contracted. Had the Commonwealth of Virginia and its political

subdivisions known of Defendants' fraudulent non-compliance, which resulted in the submission of ineligible false claims for reimbursement, they would not have paid the claims.

767. The above-named Defendants' presentment or causation of presentment, of false and/or fraudulent claims to the Commonwealth of Virginia and its political subdivisions was a foreseeable factor in the Commonwealth of Virginia and its political subdivisions' loss and a consequence of Defendants' fraudulent scheme. By virtue of the above-named Defendants' actions, the Commonwealth of Virginia and its political subdivisions have suffered damages.

2. Making or Using False Records or Statements Material to False and/or Fraudulent Claims (VA. CODE ANN. § 8.01-216.3(A)(2))

768. From at least 2012 to the present, the above-named Defendants knowingly made, used, or caused to be made or used, false records or statements material to false and/or fraudulent claims. These false, misleading, and/or fraudulent records or statements include those made on websites and in other marketing materials.

769. The above-named Defendants knowingly and fraudulently used the false statements in their marketing materials and websites both to induce the Commonwealth of Virginia and its political subdivisions to enter into the contracts and agreements at issue and to get false and/or fraudulent claims made pursuant to those contracts paid or approved by the Commonwealth of Virginia and its political subdivisions.

770. The above-named Defendants' false statements or records, or causation of false statements or records, had the potential to influence the Commonwealth of Virginia and its political subdivisions' payment decision and were material to the Commonwealth of Virginia and its political subdivisions' decision to pay the claims.

771. The above-named Defendants' false statements regarding the exclusivity and deployment models of the cloud services at issue were material because they went to the very

essence of the bargain for which the Commonwealth of Virginia and its political subdivisions contracted. Had the Commonwealth of Virginia and its political subdivisions known of Defendants' false statements regarding the cloud services at issue, which resulted in the submission of ineligible false claims for reimbursement, then the Commonwealth of Virginia and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under those contracts and agreements.

772. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated VFATA.

773. The above-named Defendants' submission, or causation of submission, of false records and statements material to false and/or fraudulent claims was a foreseeable factor in the Commonwealth of Virginia's loss and a consequence of Defendants' scheme. By virtue of Defendants' actions, the Commonwealth of Virginia and its political subdivisions have suffered damages.

3. Conspiracy (VA. CODE ANN. § 8.01-216.3(A)(3))

774. From at least 2012 to the present, the above-named Defendants conspired together to: (1) fraudulently induce the Commonwealth of Virginia and its political subdivisions to enter into contracts and agreements with them; and (2) submit or cause the submission of false and/or fraudulent claims under those contracts and agreements to the Commonwealth of Virginia and its political subdivisions.

775. Microsoft entered into agreements with the Commonwealth of Virginia and its political subdivisions that are part and parcel of the above-named Reseller Defendants' contracts with the Commonwealth of Virginia and its political subdivisions for the cloud services at issue.

776. The above-named Reseller Defendants, having issued all invoices for the specific products at issue, knew that cloud services marketed as "for Government" which utilized Microsoft's "fake SKU" included commercial cloud services, and were therefore not actually "for Government."

777. The above-named Defendants' conspiracy had the potential to influence the Commonwealth of Virginia and its political subdivisions' payment decision because the Commonwealth of Virginia and its political subdivisions would not have entered into the contracts and agreements at issue or paid claims under them had they known that they were not receiving true "government cloud" services.

* * *

778. WHEREFORE, Relator respectfully requests that the Court enter judgment against Defendants, and award the following:

To the COMMONWEALTH OF VIRGINIA:

a) Three times the amount of damages that the Commonwealth of Virginia has sustained as a result of Defendants' fraudulent and illegal practices;

b) Civil penalties against Defendants up to the maximum allowed by law for each violation of VA. CODE ANN. § 8.01-216.3; and

c) All costs incurred in bringing this action.

To RELATOR:

a) The maximum amount allowed pursuant to VA. CODE ANN. § 8.01-216.7 and/or any other applicable provision of law;

b) Reimbursement for reasonable expenses Relator incurred in connection with this action;

c) An award of reasonable attorney's fees and costs; and

d) Such further relief as this Court deems equitable and just.

Y. Count XXV – Chicago False Claims Act

779. Relator realleges and hereby incorporates by reference each and every allegation contained in all paragraphs of this complaint.

780. This is a *qui tam* action brought by Relator and the City of Chicago to recover treble damages and civil penalties under the Chicago False Claims Act ("Chicago FCA"), Chicago, Ill. Mun. Code §§ 1-21-010–1-22-060.

781. The Chicago FCA provides:

> Any person who knowingly makes a false statement of material fact to the city in violation of any statute, ordinance or regulation, or who knowingly makes a false statement of material fact to the city in connection with any application, report, affidavit, oath, or attestation, including a statement of material fact made in connection with a bid, proposal, contract or economic disclosure statement or affidavit, is liable to the city for a civil penalty of not less than $500.00 and not more than $1,000.00, plus up to three times the amount of damages which the city sustains because of the person's violation[.]

Chicago, Ill. Mun. Code § 1-21-010(a). The Chicago FCA also provides that any person who:

> (1) knowingly presents, or causes to be presented, to an official or employee of the city a false or fraudulent claim for payment or approval; [or]
> (2) knowingly makes, uses, or causes to be made or used, a false record or statement to get a false or fraudulent claim paid or approved by the city; [or]
> (3) conspires to defraud the city by getting a false or fraudulent claim allowed or paid[,]

Chicago, Ill. Mun. Code § 1-22-020(a), is liable to the City of Chicago for a civil penalty of $5,000 to $10,000, plus three times the amount of damages that the City of Chicago sustains because of the violation. *Id.*

1. False Statements of Fact (Chicago, Ill. Mun. Code § 1-21-020(a)).

782. From at least 2012 to the present, Defendants Microsoft Corporation and CDW Government, LLC knowingly made false statements of material fact to the City of Chicago ("the

City") in connection with procuring their contract to provide Microsoft cloud services, including GCC, to the City.

783. The above-named Defendants fraudulently induced the City to enter into contracts and agreements for cloud computing services by making materially false statements regarding the cloud services' government exclusivity and security. Defendants made these false statements in marketing and advertising materials and in the contracts and agreements themselves. Defendants also made false certifications in the contracts at issue as to their compliance with applicable laws, rules, ordinances, and regulations.

784. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the Chicago FCA.

785. The above-named Defendants' materially false statements had the potential to influence the City's payment decision and was material to the City's decision to pay the claims.

786. The above-named Defendants' false statements of fact regarding the cloud services at issue and their compliance with the applicable standards for cloud computing are material because they went to the very essence of the bargain for which the City contracted. Had the City known of Defendants' false statements, it would not have entered into the contracts at issue nor paid claims made under those contracts.

787. The above-named Defendants' materially false statements were a foreseeable factor in the City's loss and a consequence of Defendants' fraudulent scheme. By virtue of the above-named Defendants' actions, the City has suffered damages.

2. Presentment of False and/or Fraudulent Claims (Chicago, Ill. Mun. Code § 1-22-020(a)(1)).

788. From at least 2012 to the present, Defendants Microsoft Corporation and CDW Government, LLC knowingly presented, or caused to be presented, false and/or fraudulent claims to the City for payment or approval.

789. The above-named Defendants submitted claims for payment to the City under the contracts and agreements at issue, which were fraudulently induced.

790. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the Chicago FCA.

791. The above-named Defendants' knowing submission, or causation of submission, of false and/or fraudulent claims had the potential to influence the City's payment decision and was material to the County's decision to pay the claims.

792. The above-named Defendants' misrepresentations regarding the cloud services at issue and their compliance with the applicable standards for cloud computing are material because they went to the very essence of the bargain for which the City contracted. Had the City known of Defendants' fraudulent non-compliance, which resulted in the submission of ineligible false claims for reimbursement, it would not have paid the claims.

793. The above-named Defendants' presentment, or causation of presentment, of false and/or fraudulent claims to the City was a foreseeable factor in the City's loss and a consequence of Defendants' fraudulent scheme. By virtue of the above-named Defendants' actions, the City has suffered damages.

3. Making or Using False Records or Statements to Get False and/or Fraudulent Claims Paid or Approved by the City (Chicago, Ill. Mun. Code § 1-22-020(a)(2))

794. From at least 2012 to the present, the above-named Defendants knowingly made or used, or caused to be made or used, false records or statements in order to get false and/or fraudulent claims paid or approved by the City. These false records or statements include those made on websites and in other marketing materials.

795. The above-named Defendants knowingly and fraudulently used the false statements in their marketing materials and websites both to induce the City to enter into the contracts and agreements at issue and to get false and/or fraudulent claims made pursuant to those contracts paid or approved by the City.

796. The above-named Defendants' false statements or records had the potential to influence the City's payment decision and were material to the City's decision to pay the claims.

797. The above-named Defendants' false statements regarding the exclusivity and deployment models of the cloud services at issue were material because they went to the very essence of the bargain for which the City contracted. Had the City known of Defendants' fraudulent misrepresentations regarding the cloud services at issue, which resulted in the submission of ineligible false and/or fraudulent claims for reimbursement, then the City would not have entered into the contracts and agreements at issue or paid claims under those contracts and agreements.

798. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the Chicago FCA.

799. The above-named Defendants' creation and/or use of false records and statements were a foreseeable factor in the City's loss and a consequence of Defendants' scheme. By virtue of Defendants' actions, the City has suffered damages.

4. Conspiracy (Chicago, Ill. Mun. Code § 1-22-020(a)(3))

800. From at least 2012 to the present, the above-named Defendants conspired together to defraud the City by getting false and/or fraudulent claims paid or allowed. The above-named Defendants accomplished this by: (1) fraudulently inducing the City to enter into contracts and agreements with them; and (2) submitting or causing the submission of false and/or fraudulent claims under those contracts and agreements to the City.

801. Microsoft entered into agreements with the City that are part and parcel of Defendant CDW Government, LLC's contracts with the City for the cloud services at issue.

802. Defendant CDW Government, LLC, having issued all invoices for the specific products at issue, knew that cloud services marketed as "for Government" which utilized Microsoft's "fake SKU" included commercial cloud services, and were therefore not actually "for Government."

803. Defendants' conspiracy had the potential to influence the City's payment decision because the City would not have entered into the contracts and agreements at issue or paid claims under them had it known that it was not receiving true "government cloud" services.

* * *

804. WHEREFORE, Relator respectfully requests that the Court enter judgment against Defendants, and award the following:

To the CITY OF CHICAGO

a) Three times the amount of damages that the City of Chicago has sustained as a result of Defendants' fraudulent and illegal practices;

b) Civil penalties against Defendants up to the maximum allowed by law for each violation of Chicago, Ill. Mun. Code §§ 1-21-020(a) and 1-22-020(a); and

c) All costs incurred in bringing this action.

To RELATOR:

a) The maximum amount allowed pursuant to Chicago, Ill. Mun. Code § 1-22-030(d) and/or any other applicable provision of law;

b) Reimbursement for reasonable expenses Relator incurred in connection with this action;

c) An award of reasonable attorney's fees and costs; and

d) Such further relief as this Court deems equitable and just.

Z. Count XXVI – False Claims Ordinance of Broward County, Florida

805. Relator realleges and hereby incorporates by reference each and every allegation contained in all paragraphs of this complaint.

806. This is a *qui tam* action brought by Relator and the County of Broward to recover treble damages and civil penalties under the False Claims Ordinance of Broward County, Florida ("BCFCO"), Code of Broward County, Florida, §§ 1-276–1-287.

807. The BCFCO provides that:

> (1) Any person who knowingly presents or causes to be presented to the County, or to any officer, employee, agent, or consultant of the County, a false or fraudulent claim for payment or approval; [or]
> (2) Any person who knowingly makes, uses, or causes to be made or used, a false record or statement to get a false, fraudulent, or inflated claim paid or approved by the County; [or]
> (3) Any person who conspires to defraud the County by facilitating the payment of a false, fraudulent, or inflated claim allowed or paid by the County[,]

Code of Broward County, FL, § 1-279(a), is liable to the County of Broward for three times the part of the claim which is false, fraudulent, or inflated. Code of Broward County, FL, § 1-279(c)(1). The violator must also forfeit the entire amount of the claim and is subject to

debarment from Broward County contracting for up to five years. *See* Code of Broward County, FL, § 1-279(c).

1. Presentment of False and/or Fraudulent Claims (Code of Broward County, FL § 1-279(a)(1)).

808. From at least 2016 to the present, Defendants Microsoft Corporation and SHI International Corporation knowingly presented, or caused to be presented, false and/or fraudulent claims to Broward County for payment or approval.

809. The above-named Defendants fraudulently induced Broward County to enter into contracts and agreements for cloud computing services by making false statements regarding the cloud services' government exclusivity and security. Defendants made these false statements in marketing and advertising materials and in the contracts and agreements themselves. Defendants also made false certifications in the contracts at issue as to their compliance with applicable laws, rules, and regulations.

810. The above-named Defendants submitted claims for payment to Broward County under the contracts and agreements at issue, which were fraudulently induced.

811. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the BCFCO.

812. The above-named Defendants' knowing submission, or causation of submission, of false and/or fraudulent claims had the potential to influence Broward County's payment decision and was material to the County's decision to pay the claims.

813. The above-named Defendants' misrepresentations regarding the cloud services at issue and their compliance with the applicable standards for cloud computing are material because they went to the very essence of the bargain for which Broward County contracted. Had

Broward County known of Defendants' fraudulent non-compliance, which resulted in the submission of ineligible false claims for reimbursement, it would not have paid the claims.

814. The above-named Defendants' presentment, or causation of presentment, of false and/or fraudulent claims to Broward County was a foreseeable factor in Broward County's loss and a consequence of Defendants' fraudulent scheme. By virtue of the above-named Defendants' actions, Broward County has suffered damages.

2. Making or Using False Records or Statements to Get False, Fraudulent, and/or Inflated Claims Paid or Approved by the County (Code of Broward County, FL § 1-279(a)(2))

815. From at least 2016 to the present, the above-named Defendants knowingly made or used, or caused to be made or used, false records or statements in order to get false, fraudulent, or inflated claims paid or approved by Broward County. These false records or statements include those made on websites and in other marketing materials.

816. The above-named Defendants knowingly and fraudulently used the false statements in their marketing materials and websites both to induce Broward County to enter into the contracts and agreements at issue and to get false and/or fraudulent claims made pursuant to those contracts paid or approved by the County.

817. The above-named Defendants' false statements or records had the potential to influence Broward County's payment decision and were material to the County's decision to pay the claims.

818. The above-named Defendants' false statements regarding the exclusivity and deployment models of the cloud services at issue were material because they went to the very essence of the bargain for which Broward County contracted. Had Broward County known of Defendants' fraudulent misrepresentations regarding the cloud services at issue, which resulted

in the submission of ineligible false and/or fraudulent claims for reimbursement, then Broward County would not have entered into the contracts and agreements at issue or paid claims under those contracts and agreements.

819. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the BCFCO.

820. The above-named Defendants' creation and/or use of false records and statements were a foreseeable factor in Broward County's loss and a consequence of Defendants' scheme. By virtue of Defendants' actions, Broward County has suffered damages.

3. Conspiracy (Code of Broward County, FL § 1-279(a)(3))

821. From at least 2016 to the present, Defendants Microsoft Corporation and SHI International Corporation conspired together to defraud Broward County by facilitating the payment of false, fraudulent, and/or inflated claims allowed or paid by the County. The above-named Defendants accomplished this by: (1) fraudulently inducing Broward County to enter into contracts and agreements with them; and (2) submitting or causing the submission of false and/or fraudulent claims under those contracts and agreements to Broward County.

822. Microsoft entered into agreements with Broward County that are part and parcel of Defendant SHI International Corporation's contracts with Broward County for the cloud services at issue.

823. Defendant SHI International Corporation, having issued all invoices for the specific products at issue, knew that cloud services marketed as "for Government" which utilized Microsoft's "fake SKU" included commercial cloud services, and were therefore not actually "for Government."

824. Defendants' conspiracy had the potential to influence Broward County's payment decision because the County would not have entered into the contracts and agreements at issue or paid claims under them had it known that it was not receiving true "government cloud" services.

* * *

825. WHEREFORE, Relator respectfully requests that the Court enter judgment against Defendants, and award the following:

To BROWARD COUNTY, FLORIDA

a) Three times the amount of claims Defendants submitted to Broward County that are false, fraudulent, and/or inflated;

b) Civil penalties against Defendants up to the maximum allowed by law for each violation of the Code of Broward County, Florida § 1-279(a); and

c) All costs incurred in bringing this action.

To RELATOR:

a) The maximum amount allowed pursuant the Code of Broward County, Florida § 1-282 and/or any other applicable provision of law;

b) An award of reasonable attorney's fees and costs; and

c) Such further relief as this Court deems equitable and just.

AA. Count XXVI – Miami-Dade County False Claims Ordinance

826. Relator realleges and hereby incorporates by reference each and every allegation contained in all paragraphs of this complaint.

827. This is a *qui tam* action brought by Relator and Miami-Dade County, Florida to recover treble damages under the Miami-Dade County False Claims Ordinance ("MDFCO"), Code of Miami-Dade County, Florida §§ 21-255–21-266.[33]

828. The MDFCO provides:

[33] *Available at* http://www.miamidade.gov/govaction/matter.asp?matter=992791&file=false&yearFolder=Y1999

> (a) Any person who knowingly presents or causes to be presented to the County, or to any office, employee, agent, or consultant of the County, a false or fraudulent claim for payment or approval; [or]
> (b) Any person who knowingly makes, uses, or causes to be made or used, a false record or statement to get a false, fraudulent, or inflated claim paid or approved by the County; [or]
> (c) Any person who conspires to defraud the County by facilitating the payment of a false, fraudulent, or inflated claim paid or approved by the County[,]

Code of Miami-Dade County, FL § 21-258(1), is liable to Miami-Dade County ("the County") for an amount equal to three times that part of the claim which is false, fraudulent, or inflated, as well as all costs and fees incurred by the County in reviewing, defending, and evaluating the claim. Code of Miami-Dade County, FL § 21-258(3). The violator is also required to "immediately, fully, and irrevocably forfeit the entire amount of the claim" and will be debarred from contracting with the County for five years or less. *Id.*

1. Presentment of False and/or Fraudulent Claims (Code of Miami-Dade County, FL § 21-258(1)(a)).

829. From at least 2016 to the present, the following Defendants knowingly presented, or caused to be presented, false and/or fraudulent claims to Miami-Dade County: Microsoft Corporation; Insight Public Sector, Inc.; and SHI International Corporation.

830. The above-named Defendants fraudulently induced Miami-Dade County to enter into contracts and agreements for cloud computing services by making false statements regarding the cloud services' government exclusivity and security. Defendants made these false statements in marketing and advertising materials as well as in the contracts and agreements themselves.

831. The above-named Defendants submitted claims for payment to Miami-Dade County under the contracts and agreements at issue, which were fraudulently induced.

832. The above-named Defendants also made false certifications in the contracts and agreements at issue as to their compliance with applicable laws.

833. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the MDFCO.

834. The above-named Defendants' knowing submission, or causation of submission, of false and/or fraudulent claims had the potential to influence Miami-Dade County's payment decision and was material to the County's decision to pay the claims.

835. The above-named Defendants' misrepresentations regarding the cloud services at issue and their compliance with the applicable standards for cloud computing are material because they went to the very essence of the bargain for which Miami-Dade County contracted. Had Miami-Dade County known of Defendants' fraudulent non-compliance, which resulted in the submission of ineligible false claims for reimbursement, it would not have paid the claims.

836. The above-named Defendants' presentment, or causation of presentment, of false and/or fraudulent claims to Miami-Dade County was a foreseeable factor in Miami-Dade County's loss and a consequence of Defendants' fraudulent scheme. By virtue of the above-named Defendants' actions, Miami-Dade County has suffered damages.

2. Making or Using False Records or Statements to Get False and/or Fraudulent Claims Paid or Approved by the County (Code of Miami-Dade County, FL § 21-258(1)(b))

837. From at least 2016 to the present, the above-named Defendants knowingly made or used false records or statements in order to get false and/or fraudulent claims paid or approved by Miami-Dade County. These false records or statements include those made on websites and in other marketing materials.

838. The above-named Defendants knowingly and fraudulently used the false statements in their marketing materials and websites both to induce Miami-Dade County to enter

into the contracts and agreements at issue and to get false and/or fraudulent claims made pursuant to those contracts paid or approved by the County.

839. The above-named Defendants' false statements or records had the potential to influence Miami-Dade County's payment decision and were material to the County's decision to pay the claims.

840. The above-named Defendants' false statements regarding the exclusivity and deployment models of the cloud services at issue were material because they went to the very essence of the bargain for which Miami-Dade County contracted. Had Miami-Dade County known of Defendants' fraudulent misrepresentations regarding the cloud services at issue, which resulted in the submission of ineligible false and/or fraudulent claims for reimbursement, then Miami-Dade County would not have entered into the contracts and agreements at issue or paid claims under those contracts and agreements.

841. By creating and carrying out their fraudulent scheme, the above-named Defendants knowingly and repeatedly violated the MDFCO.

842. The above-named Defendants' creation and/or use of false records and statements were a foreseeable factor in Miami-Dade County's loss and a consequence of Defendants' scheme. By virtue of Defendants' actions, Miami-Dade County has suffered damages.

3. Conspiracy (Code of Miami-Dade County, FL § 21-258(1)(c))

843. From at least 2016 to the present, the above-named Defendants conspired together to: (1) fraudulently induce Miami-Dade County to enter into contracts and agreements with them; and (2) submit or cause the submission of false and/or fraudulent claims under those contracts and agreements to Miami-Dade County.

844. Microsoft entered into agreements with Miami-Dade County that are part and parcel of the Reseller Defendants' contracts with Miami-Dade County for the cloud services at issue.

845. Defendants Insight Public Sector, Inc. and SHI International Corporation, having issued all invoices for the specific products at issue, knew that cloud services marketed as "for Government" which utilized Microsoft's "fake SKU" included commercial cloud services, and were therefore not actually "for Government."

846. Defendants' conspiracy had the potential to influence Miami-Dade County's payment decision because the County would not have entered into the contracts and agreements at issue or paid claims under them had it known that it was not receiving true "government cloud" services.

* * *

847. WHEREFORE, Relator respectfully requests that the Court enter judgment against Defendants, and award the following:

To MIAMI-DADE COUNTY, FLORIDA:

a) Three times the amount of damages that Miami-Dade County has sustained as a result of Defendants' fraudulent and illegal practices;

b) Civil penalties against Defendants up to the maximum allowed by law for each violation of the Code of Miami-Dade County, Florida § 21-258(1); and

c) All costs incurred in bringing this action.

To RELATOR:

a) The maximum amount allowed pursuant to the Code of Miami-Dade County, Florida § 21-261 and/or any other applicable provision of law;

b) An award of reasonable attorney's fees and costs; and

c) Such further relief as this Court deems equitable and just.

XII. DEMAND FOR JURY TRIAL

848. Pursuant to Federal Rule of Civil Procedure 38, Relator demands a trial by jury.

XIII. DOCUMENTARY EVIDENCE

849. The documentary evidence referenced herein consists of the following:

Exhibit No.	Description	Bates Numbers
1	E-mail from Relator to Roger Singh & David Case (June 23, 2017)	KFE000001–KFE000009
2	Pension Benefit Guaranty Corporation Contract GS-35F-0111K (Apr. 1, 2015)	KFE000010–KFE000047
3	National Institute of Standards and Technology Special Publication 800-145 (2011)	KFE000048–KFE000054
4	Pension Benefit Guaranty Corporation Contract GS-35F-0195J (Sept. 30, 2011)	KFE000055–KFE000067
5	FBI Criminal Justice Information Systems Recommendations for Implementation of Cloud Computing Solutions (Aug. 10, 2012)	KFE000068–KFE000136
6	Microsoft Azure Government Overview Document (Dec. 2014)	KFE000137–KFE000168
7	Microsoft Azure Government Information Sheet (2016)	KFE000169–KFE000170
8	Microsoft Azure Government PowerPoint (June 29, 2016)	KFE000171–KFE000177
9	Office 365 US Government Service Descriptions (Feb. 14, 2017)	KFE000178–KFE000194
10	Microsoft Ignite PowerPoint (Sept. 2017)	KFE000195–KFE000231
11	Office 365 Government Service Plans Description (Oct. 16, 2017)	KFE000232–KFE000241
12	California Statewide Dell Contract	KFE000242–KFE000380
13	Microsoft Azure Government Contact Form	KFE000381
14	Los Angeles County Community Development Commission Contract (Sept. 1, 2015)	KFE000382–KFE000419
15	Relator's September 2016 Connect Evaluation	KFE000420–KFE000435
16	E-mail from Relator to Adrian Michels, Michael Nicosia, & Kristie Atwood (Sept. 2, 2016)	KFE000436–KFE000439
17	E-mail Chain between Relator, Rue Limones, & Others (Oct. 13, 2016)	KFE000440–KFE000452
18	E-mail from Relator to Roger Singh (Jan. 17, 2017)	KFE000453–KFE000458
19	E-mail Chain between Relator, Roger Singh, & Others (Jan. 22, 2017)	KFE000459–KFE000461
20	E-mail Chain between Relator, Roger Singh, & Kevin Bognar (Feb. 3, 2017)	KFE000462–KFE000466

Exhibit No.	Description	Bates Numbers
21	E-mail Chain between Relator, Phil West, & Others (Jan. 31, 2017)	KFE000467–KFE000473
22	E-mail Chain between Relator & Roger Singh (Feb. 3, 2017)	KFE000474–KFE000477
23	E-mail Chain between Relator & John Kelbley (Feb. 16, 2017)	KFE000478–KFE000483
24	E-mail Chain between Relator & Roger Singh (Feb. 17, 2017)	KFE000484–KFE000485
25	E-mail Chain between Relator, Scott Villinski, & Others (Feb. 21, 2017)	KFE000486–KFE000489
26	Relator's February 2017 Connect Evaluation	KFE000490–KFE000506
27	E-mail Chain between Relator & Adam Baron (Mar. 31, 2017)	KFE000507–KFE000511
28	E-mail Chain between Relator, Brandon Meyer, & Others (Apr. 3, 2017)	KFE000512–KFE000516
29	E-mail Chain between Relator & Singh (May 24, 2017)	KFE000517–KFE000518
30	Relator's June 2017 Connect Evaluation	KFE000519–KFE000545
31	E-mail Chain between Relator, Singh, & Others (June 7, 2017)	KFE000546–KFE000553
32	Relator's Termination Letter (July 6, 2017)	KFE000554–KFE000556
33	E-mail Chain between Relator & Bharat Shah (July 6, 2017)	KFE000557–KFE000562
34	CA orange county	KFE000563–KFE000630
35	Azure Government Slide with Speaker Notes (2012)	KFE000631
36	E-mail Chain between Relator, Bharat Shah, & Dan Plastina (July 6, 2017)	KFE000632–KFE000642
37	Stanislaus County, California Contracts & Agreements (2017)	KFE000643–KFE000761
38	NASPO Multistate Contract (2016)	KFE000762–KFE000819
39	Florida Statewide Contract 43230000-15-2 (2016)	KFE000820–KFE000852
40	Pinellas County, Florida Contract & Agreements (2015)	KFE000853–KFE000881
41	City of Miramar, Florida Contract (2015)	KFE000882–KFE001009
42	Chicago, Illinois & Illinois Statewide Contract & Agreements (2012)	KFE001010–KFE001086
43	Bloomington, Illinois & Illinois Statewide Contract	KFE001087–KFE001123
44	Iowa Statewide and Fairfax County, Virginia Contract (2016)	KFE001124–KFE001247
45	Los Alamos County, New Mexico Contract & Agreements (2014)	KFE001248–KFE001269
46	Memphis, Tennessee & Tennessee Statewide Contract (2015)	KFE001270–KFE001307
47	Virginia Statewide Contract VA-070907-SHI (2010)	KFE001308–KFE001342
48	Virginia Statewide Contract VA-131017-SHI (2013)	KFE001343–KFE001392

Exhibit No.	Description	Bates Numbers
49	2015 Los Angeles County Microsoft Agreements	KFE001393–KFE001436
50	Los Angeles County Community Development Commission Contract (May 23, 2016)	KFE001437–KFE001474
51	San Bernardino County, California Terms and Conditions (June 28, 2011)	KFE001475–KFE001476
52	Microsoft Agreements for Florida Statewide Contract 43230000-15-2 (2016)	KFE001477–KFE001500
53	E-mail Chain between Relator, Phil West, & Others (Oct. 21–25, 2016)	KFE001501–KFE001505
54	GCC OneList Issue Tracker (Sept. 16, 2015)	KFE001506–KFE001507
55	Minnesota Microsoft Enrollment Agreements (Mar. 3, 2015)	KFE001508–KFE001546
56	Manatee County, Florida Microsoft Agreements	KFE001547–KFE001574
57	City of Sparks, Nevada Microsoft Enterprise Enrollments	KFE001575–KFE001590
58	Vallejo, California Microsoft Agreement	KFE001591–KFE001607
59	Los Angeles County Community Development Commission Server & Cloud Enrollment Agreement (June 21, 2016)	KFE001608–KFE001628
60	City of Wilmington, Delaware Microsoft Agreements (2018)	KFE001629–KFE001650
61	Nassau County, Florida Microsoft Agreements (2017)	KFE001651–KFE001669
62	City of Jupiter, Florida Contract Information & Microsoft Agreements (2016)	KFE001670–KFE001691
63	Las Vegas Metropolitan Police Department Microsoft Agreements (2016)	KFE001692–KFE001713
64	Ravalli County, Montana Contract Information & Microsoft Agreements (2015)	KFE001714–KFE001746
65	City of Memphis, Tennessee Microsoft Agreements (2015)	KFE001747–KFE001764
66	E-mail Chain between Relator, John Kelbley, & Others (Jan. 24, 2017)	KFE001765–KFE001768
67	Microsoft CJIS Implementation Guidelines (July 2016)	KFE001769–KFE001783

Respectfully submitted,

Joel M. Androphy
NY State Bar No. 4578142
Rebecca L. Gibson
Pending *pro hac vice* admission

TX State Bar No. 24092418
Chris Sprengle
NY State Bar No. 4287686

BERG & ANDROPHY
120 West 45th Street
Suite 3801
New York, NY 10036
Tel. (713) 529-5622
Fax (713) 529-3785
jandrophy@bafirm.com
rgibson@bafirm.com

COUNSEL FOR RELATOR JOHN KURZMAN

CERTIFICATE OF SERVICE

I hereby certify that on May 10, 2019, a true and correct copy of this Original Complaint was delivered to the following individuals via certified mail, return receipt requested:

Civil-Process Clerk U.S. Attorney's Office Southern District of New York 86 Chambers Street, 3rd Floor New York, NY 10007	William Barr United States Attorney General Department of Justice 950 Pennsylvania Ave. N.W. Washington, DC 20530
Karl A. Racine District of Columbia Attorney General 441 4th Street Northwest Washington, DC 20001	Xavier Becera Attorney General of California California Department of Justice 1300 I Street Sacramento, CA 95814-2919
Kathy Jennings Delaware Attorney General 820 North French Street Wilmington, DE 19801	Ashley Moody Florida Attorney General The Capitol PL-01 Tallahassee, FL 32399-0001
Jim Patronis, Chief Financial Officer Florida Department of Financial Services 200 East Gaines Street Tallahassee FL 32399	Clare E. Connors Hawaii Attorney General 425 Queen Street Honolulu, HI 96813
Joseph K. Kamelamela Corporation Counsel, County of Hawaii 101 Aupuni Street, Unit 325 Hilo, HI 96720	Paul S. Aoki, Acting Corporation Counsel City & County of Honolulu 530 South King Street, Room 110 Honolulu, HI 96813
Moana M. Lutey Acting Corporation Counsel, County of Maui 200 South High Street, 3rd Floor Wailuku, HI 96793	Kwame Raoul Attorney General of Illinois Illinois Office of the Attorney General 100 W. Randolph St. Chicago, IL 60601
Curtis Hill Attorney General of Indiana Indiana Office of the Attorney General 302 W. Washington Street, 5th Floor Indianapolis, IN 46204	Lori Torres Indiana Inspector General 315 West Ohio Street, Room 104 Indianapolis, IN 46202
Maura Healey Massachusetts Attorney General 1 Ashburton Place, Suite 1801 Boston, MA 02108-1518	Keith Ellison Minnesota Attorney General 1400 Bremer Tower 445 Minnesota Street St. Paul, MN 55101

Tim Fox Montana Attorney General 215 North Sanders, 3rd Floor Helena, MT 59620-1401	Aaron Ford Nevada Attorney General Old Supreme Court Building 100 North Carson Street Carson City, NV 89701-4717
Gurbir S. Grewal New Jersey Attorney General's Office 25 Market Street Trenton, NJ 08625-0080	Hector Balderas New Mexico Attorney General 408 Galisteo Street Santa Fe, NM 87501
Josh Stein Attorney General of North Carolina NC Department of Justice 114 West Edenton Street Raleigh, NC 27603	Herbert Slatery III Tennessee Attorney General & Reporter War Memorial Building 301 6th Avenue North Nashville, TN 37243
Mark Herring Virginia Attorney General 202 North 9th Street Richmond, VA 23219	Anna M. Valencia Chicago City Clerk 121 North LaSalle Street, Room 107 Chicago, IL 60602
Edward N. Siskel Chicago Corporation Counsel 121 North LaSalle Street, Suite 600 Chicago, IL 60602	Bertha W. Henry Broward County Administrator 115 South Andrews Avenue, Room 409 Fort Lauderdale, FL 33301
Alina T. Hudak Miami-Dade County Manager 111 NW 1st Street, Suite 2910 Miami, FL 33128	

I further certify that on May 10, 2019, a true and correct copy of this Original Complaint was personally served on:

- Tom Miller, Iowa Attorney General, 1305 East Walnut Street, Floor 2, Des Moines, IA 50319;
- Peter Neronha, Rhode Island Attorney General, 150 South Main Street, Providence, RI 02903; and
- T.J. Donovan, Vermont Attorney General, 109 State Street, Montpelier, VT 05609.

Rebecca L. Gibson

Glossary of Acronyms

AAD: Azure Active Directory. Manages user identities (usernames and passwords) for all Azure cloud services, including the Government Community Cloud ("GCC") services at issue. The GCC iteration of AAD operates in the commercial cloud.

AADP: Azure Active Directory Premium. An "upgrade" to standard AAD (AAD Basic) which GCC customers paid more to receive.

AIP: Azure Information Protection. Secure Islands product acquired by Microsoft

AzGov: Microsoft Azure Government.

CAS: Cloud Application Security. Adallom product acquired by Microsoft.

CJIS: Criminal Justice Information Systems. A division of the FBI that issues standard protocol for evaluating security for cloud services. Microsoft has signed CJIS agreements (certifying compliance) with many states, including the Government Plaintiff states of California, Florida, Hawaii, Illinois, Indiana, Iowa, Minnesota, Montana, New Jersey, Nevada, North Carolina, Rhode Island, Tennessee, and Vermont, as well as the Commonwealths of Massachusetts and Virginia.

CMS: Centers for Medicare and Medicaid Services, a U.S. federal government agency.

DoD: United States Department of Defense, a U.S. federal government agency.

EMS: Enterprise Mobility & Security Suite. Includes AIP and CAS, among other products and services.

FCA: federal False Claims Act

FCC: Federal Communications Commission, a U.S. federal government agency.

FED: Federal business sector (Microsoft internal terminology).

FedRAMP: Federal Risk and Authorization Management Program. Federal government-wide program providing a standardized approach to assessing security for cloud services. Has two relevant categories of certification, "High" and "Moderate" – each is for different risk categories of information.

GBB: Global Black Belt (Microsoft internal terminology) – an "expert" on a specific product or product suite.

GCC: Government Community Cloud. The "fake" government cloud services at issue, which partially operate and store data in the commercial cloud.

GOV: Abbreviation used to denote government products at Microsoft (i.e. AZUREGOV, AZGOV, etc.).

HUD: United States Department of Housing and Urban Development, a U.S. federal government agency.

MAG: Microsoft Azure Government.

NIST: National Institute of Standards and Technology. Government agency that, among other things, sets out standardized definitions and guidelines for cloud computing.

O365: Microsoft Office 365.

PANYNJ: Port Authority of New York and New Jersey.

RMS: Rights Management System. Microsoft's encryption technology; used by AIP to perform encryption. Operates outside of the government cloud, in the Azure commercial cloud.

SLG: State & Local Government business sector (Microsoft internal terminology).

SPE: Secure Productive Enterprise. This is a "suite" of products and services that consists of Microsoft Azure, EMS, and Windows 10.

USAID: United States Agency for International Development, a U.S. federal government agency.

USPS: United States Postal Service, a U.S. federal government agency.

VITA: Virginia Information Technology Agency, a government agency of the Commonwealth of Virginia.